



Course Presentation

CCNA

(Cisco Certified Network Associate)

Certification Mapped Course

Routing and Switching

Course Presentation



© 2015 ZOOM Technologies India Pvt. Ltd.

All rights reserved. No part of this book or related material may be reproduced in any form or by any means without prior permission from Zoom Technologies India Pvt. Ltd. All precautions have been take to make this book and related material error-free. However, Zoom Technologies India Pvt. Ltd. is not liable for any errors or omissions. The contents of this book are subject to change without notice.

DISCLAIMER: CISCO, CCNA, CATALYST are registered trademarks of Cisco Inc.



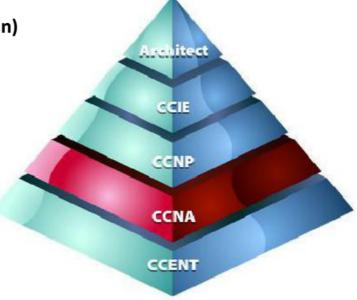


CERTIFICATIONS



- Cisco certifications are globally respected IT certification programs for Wide Area Networking (Internetworking).
- · Cisco has five levels of certification:
 - CCENT (Cisco Certified Entry Networking Technician)
 - CCNA (Cisco Certified Network Associate)
 - CCNP (Cisco Certified Network Professional)
 - CCIE (Cisco Certified Internetworking Expert)
 - CCAr (Cisco Certified Architect)

room





CCNA Certification Track



There are 2 tracks for CCNA examination:

- Two paper track
 - ICND 1 (100-101) (On passing this exam the candidate is CCENT)
 - ICND 2 (200-101) (On passing both exams the candidate is CCNA)

OR

- One paper track
 - CCNA (200-120) (On passing this exam the candidate is CCNA)





CCNA Certification



 Cisco Certified Network Associate R&S exam is the associate level exam into Wide Area Networking.

Exam Number : 200-120 CCNAX

Duration : 90 Minutes

Number of questions : 50-60 questions

Passing Mark : 825 / 1000

Available Languages : English

Exam Questions : Multiple-choice single answer

Multiple-choice multiple answer

Drag-and-drop

Simulations (Simlet)

Scenario Based (Testlet)

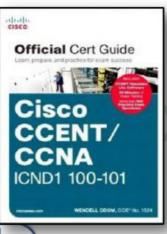


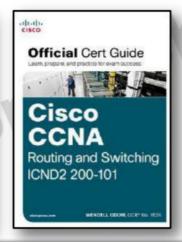
Reference Books

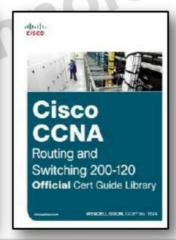


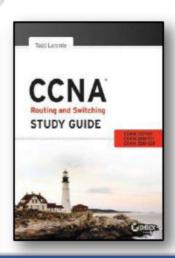
- CCNA ICND 1 (100-101) Wendell Odom Cisco Press
- CCNA ICND 2 (200-101) Wendell Odom Cisco Press
 OR
- CCNA Study Guide (200-120) Todd Lamle

oom



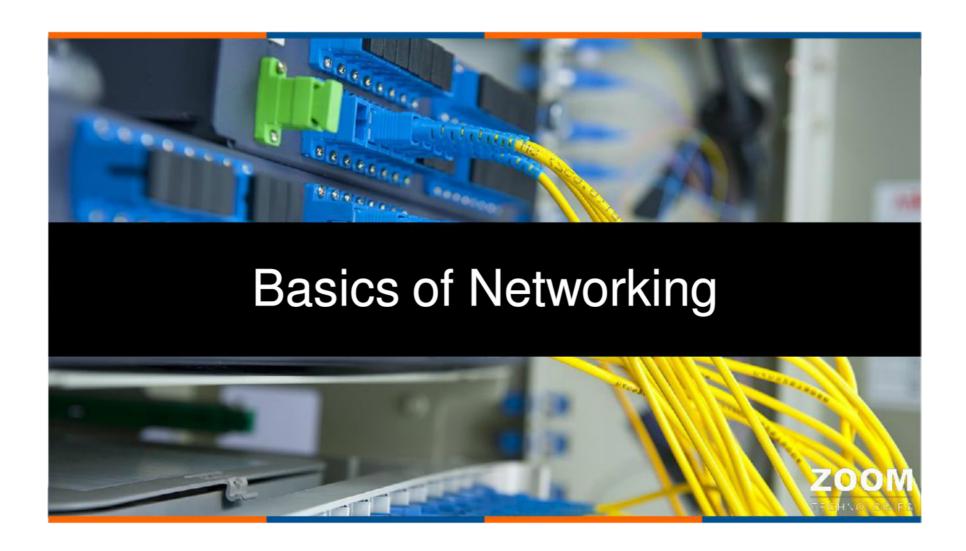












Network



- · Interconnection of two or more devices is called as a network.
- The communication between two or more interconnected devices is called networking.
- · An internetwork is a connection of two or more networks.

Zoom

• Internetworking means communication between different networks.



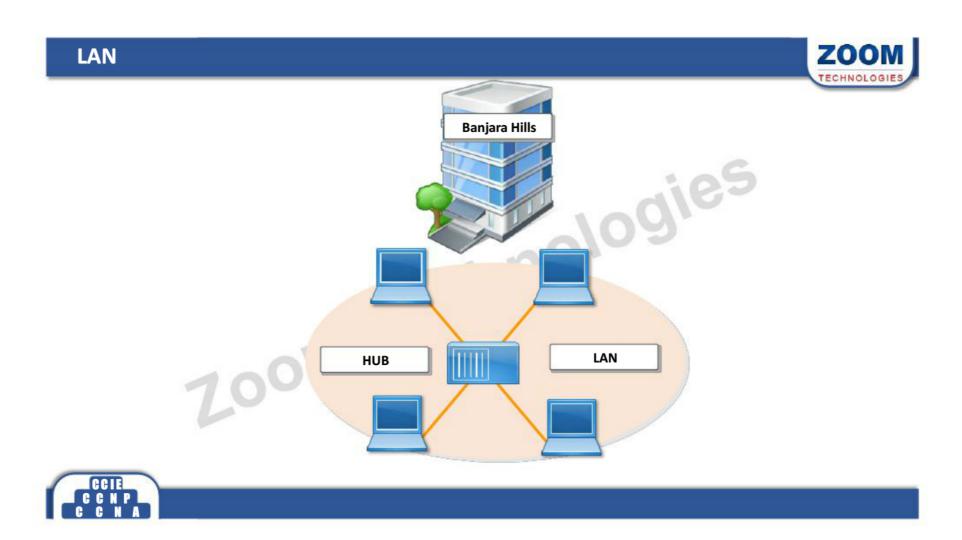


Types of Networks

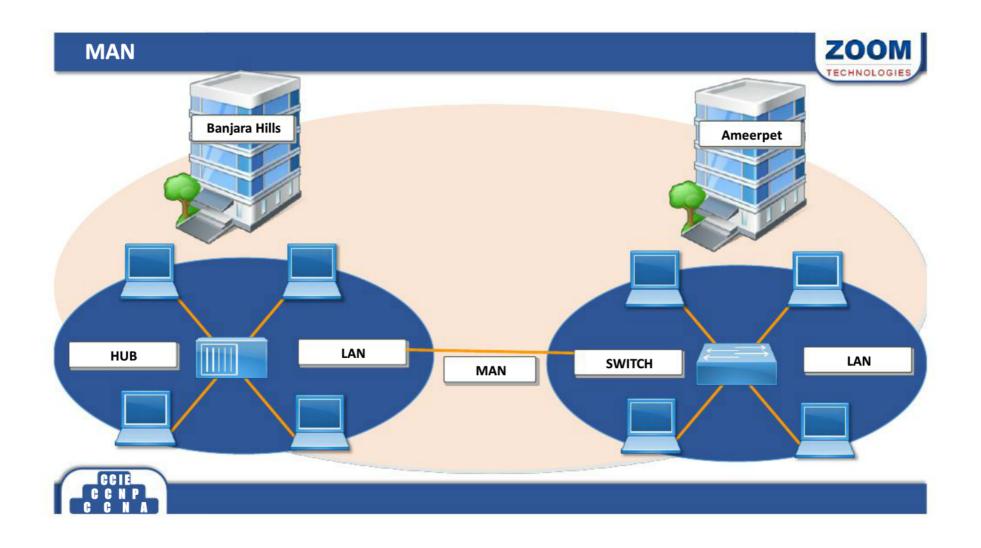


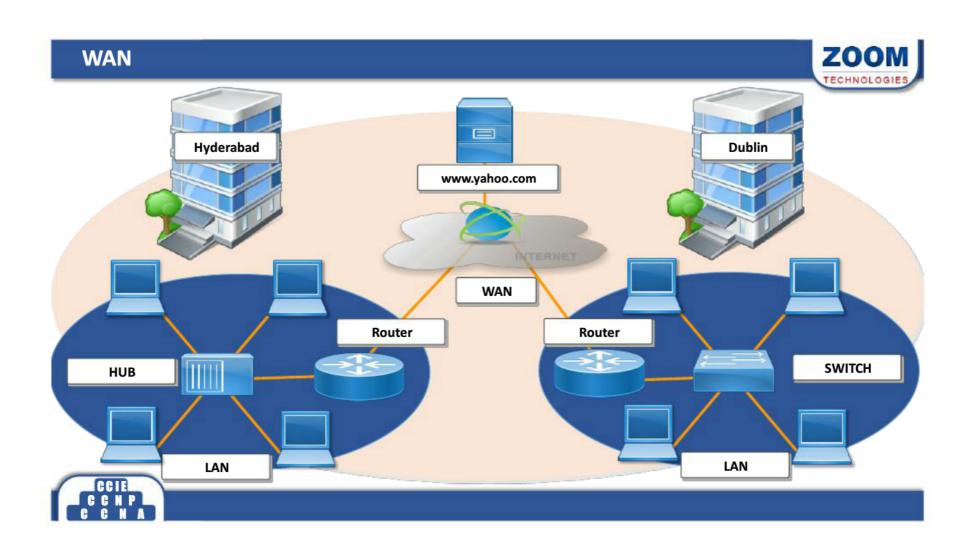
- LAN
 - Local Area Networks are used to connect networking devices that are in a very close geographic area such as a floor of a building, a building itself or within a campus.
- MAN
 Metropolitan Area Network are used to connect networking devices that may span around the entire city.
- WAN
 Wide Area Networks which connects two or more LANs present at different geographical locations.













Basic requirements to form a network



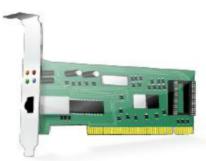
- NIC (Network interface card) also called as LAN card
- Media
- ress) rechnologies Networking devices (Hub, Switch, Router etc.)
- Protocols
- Logical Address (IP address)



NIC(Network Interface Card)



- NIC is the interface between the computer and the network
- It is also known as the Lan card or Ethernet card
- Ethernet cards have a unique 48 bit address called as MAC (Media access control) address
 - MAC address is also called as Physical address or hardware address
 - The 48 bit MAC address is represented as 12 Hexa-decimal digits
 - Example: 0016.D3FC.603F
- Network cards are available in different speeds
 - Ethernet (10 Mbps)
 - Fast Ethernet (100 Mbps)
 - Gigabit Ethernet (1000 Mbps)



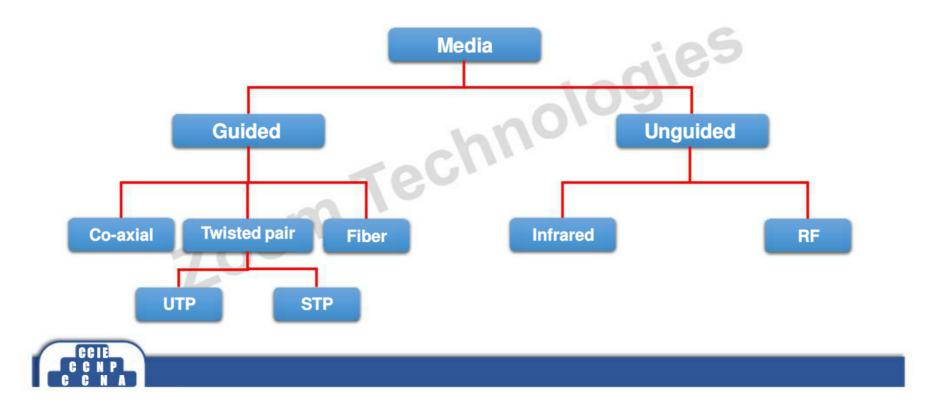


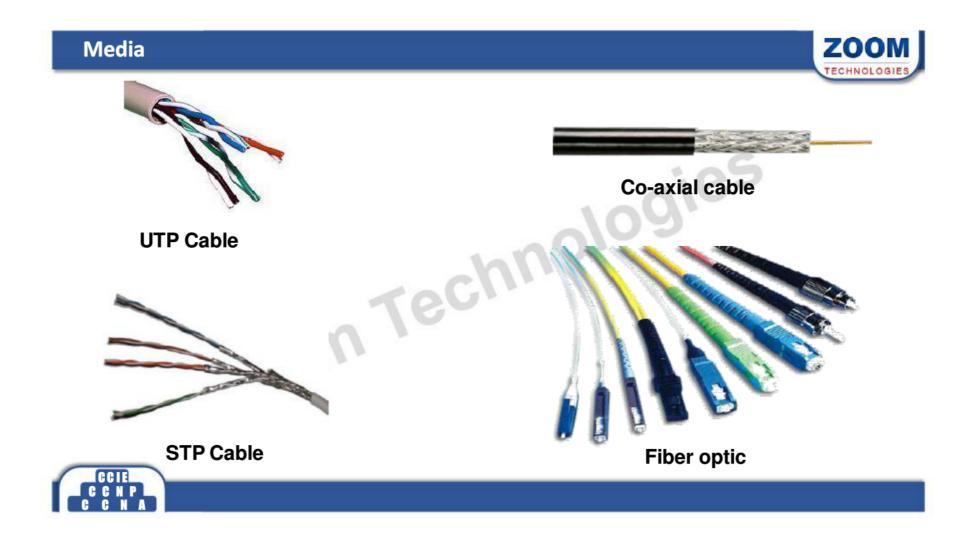


Media



• The purpose of the media is to transport bits from one machine to another.





Types of Twisted Pair cables



Category	DTR	Purpose	Connector
CAT 1	1 Mbps	Telephone Lines	RJ 11
CAT 2	4 Mbps		RJ 11
CAT 3	10 Mbps	Ethernet	RJ 45
CAT 4	16 Mbps		RJ 45
CAT 5	100 Mbps	Fast Ethernet	RJ 45
CAT 5e	500 Mbps		RJ 45
CAT 6	1000 Mbps	Gigabit Ethernet	RJ 45



Topology



Topology is a physical layout of the systems connected in a network.

Zoom Technologies Different types of topology are:

- Bus
- Ring
- Mesh
- Star

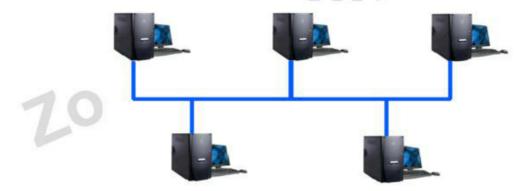




Bus Topology



- In bus topology all devices are connected to a single cable or backbone.
- It supports half duplex communication.
- A break at any point along the backbone will result in total network failure.

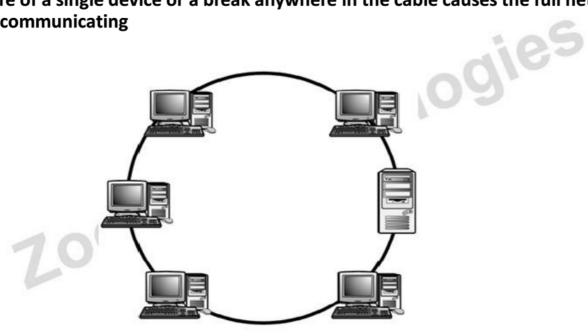




Ring Topology



- In ring topology each computer or device is connected to its neighbor forming a loop.
- Failure of a single device or a break anywhere in the cable causes the full network to stop communicating



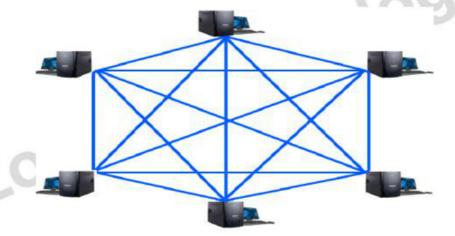




Mesh Topology



- · In mesh topology each device is directly connected to all other devices
- The disadvantage is the number of NIC's required on each device and the complex cabling.

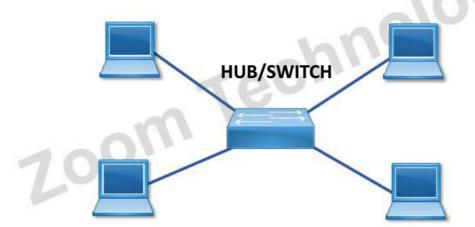




Star Topology



- The most commonly used topology
- It consist of one centralized device which can be either a switch or a hub.
- The devices connect to the various ports on the centralized devices.







Networking devices



The various types of networking devices are:

- Hub
- Switch
- Zoom Technologies Router



Hub / Repeater



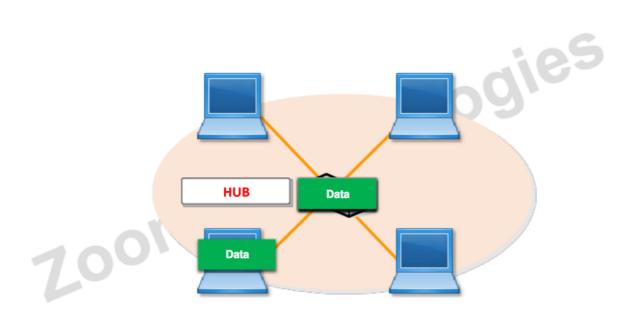
- It is not an Intelligent Device.
- It works with bits.
- zoom zechnologies Zoom Uses broadcast for communication.
- Bandwidth is shared.
- Half-duplex communication.





Functions of HUB

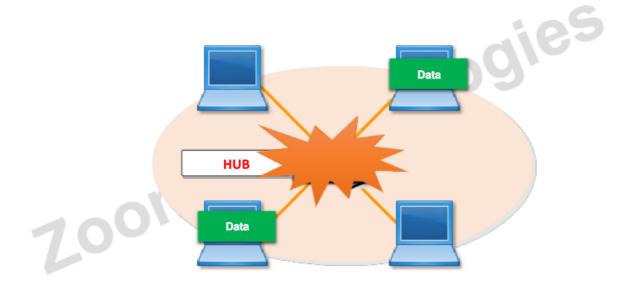






Functions of HUB









Switch

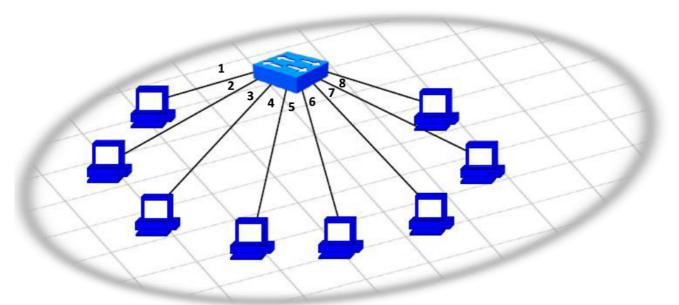


- It is an Intelligent device.
- chnologies • It maintains MAC address table (hardware address).
- Each port of the switch has fixed bandwidth.
- It works with Flooding and Unicast.
- Supports full duplex communication 200M



Functions of Switch



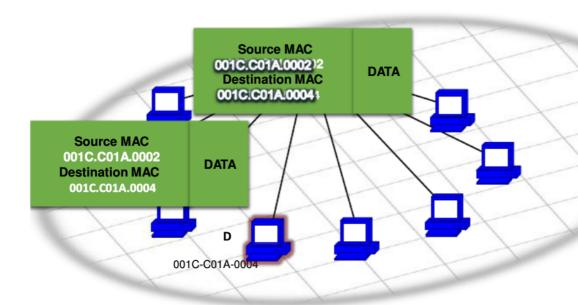






Functions of Switch



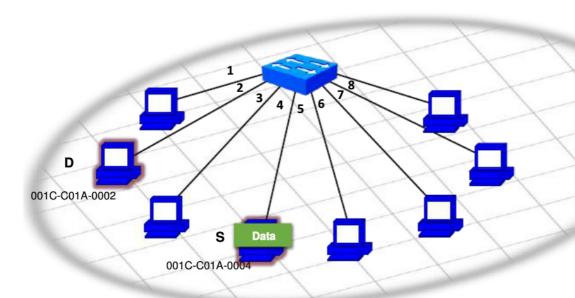


MAC	ADDRESS TABLE
PORT	MAC-ADDRESS
1	
2	001C-C01A-0002
3	
4	
5	
6	
7	
8	



Functions of Switch





	MA	C ADDRESS TABLE
	PORT	MAC-ADDRESS
1	Fa0/1	
	Fa0/2	001C-C01A-0002
	Fa0/3	
1	Fa0/4	001C-C01A-0004
	Fa0/5	
	Fa0/6	
	Fa0/7	
	Fa0/8	





Router



- It is an Intelligent device
- It works with Logical Addressing (i.e. IP, IPX, AppleTalk)
- · It works with Fixed bandwidth

Symbolic Representation:

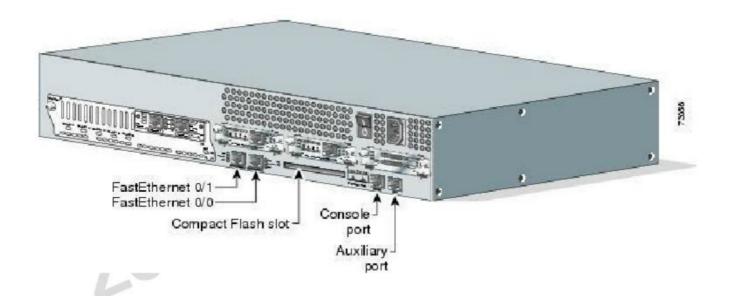
7.00m T





ROUTER









Interconnecting Network Devices



	PC	HUB	Bridge	Switch	Router
PC	Cross Cable	Straight	Cross Cable	Straight	Cross Cable
нив	Straight	Cross Cable	Straight	Cross	Straight
Bridge	Cross Cable	Straight	Cross Cable	Straight	Cross Cable
Switch	Straight	Cross	Straight	Cross Cable	Straight
Router	Cross Cable	Straight	Cross Cable	Straight	Cross Cable







OSI



- OSI was developed by the International Organization for Standardization (ISO) and introduced in 1984.
- It is a layered architecture (consists of seven layers).
- Each layer defines a set of functions which takes part in data communication.



OSI Model Layers



Layer - 7	Application	User support Layers
Layer - 6	Presentation	or O
Layer - 5	Session	Software Layers
Layer - 4	Transport	Core layer of the OSI
Layer - 3	Network)
Layer - 2	Data Link	Network support Layers
Layer - 1	Physical	or Hardware Layers





Application Layer



Application

Presentation

Session

Transport

Network

Data Link

Physical

Application Layer: is responsible for providing an interface for the users to interact with application services or Networking Services.

Ex: Web browser(HTTP), Telnet etc.



Examples of Networking Services



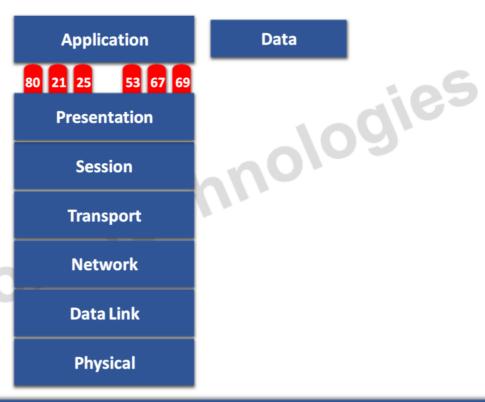
Service	Port No.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69





Data flow from Application Layer





Data



Presentation Layer



Application
Presentation
Session
Transport
Network
Data Link
Physical

Presentation Layer: It is responsible for defining a standard format to the data.

It deals with data presentation.

The major functions described at this layer are..

Encoding Decoding

ASCII, EBCDIC (Text)

JPEG,GIF,TIFF (Graphics)

MIDI, WAV (Voice)

MPEG, DAT, AVI (Video)

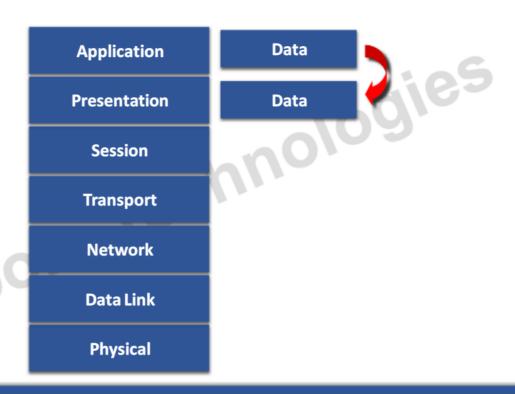
Encryption – Decryption

Compression – Decompression



Data flow from Presentation Layer







Session Layer



Application
Presentation
Session
Transport
Network
Data Link
Physical

Session Layer: It is responsible for establishing, maintaining and terminating the sessions.

Session ID is used to identify a session or interaction.

Ex:

RPC Remote Procedural Call

SQL Structured Query Language

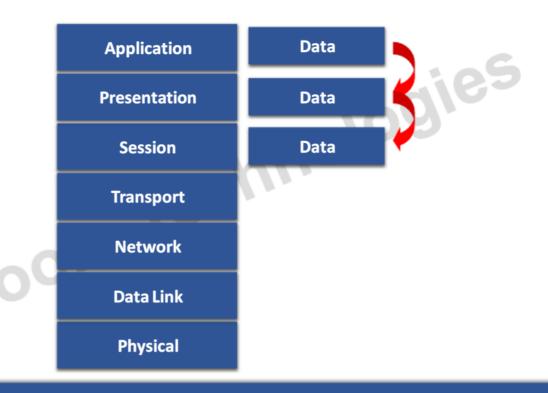
ASP AppleTalk Session protocol





Data flow from Session Layer







Transport Layer



	Application	
	Presentation	
	Session	
	Transport	
	Network	
	Data Link	
	Physical	
TE .		

Transport Layer: It provides data delivery mechanism between the applications in the network.

The major functions described at the Transport Layer are.

- •Identifying Service
- Multiplexing & De-multiplexing
- Segmentation
- Sequencing & Reassembling
- •Error Correction
- Flow Control



Identifying a Service



- Identification of Services is done using port Numbers.
- .±151 49152 65535 · Port is a logical communication Channel

Total No. Ports

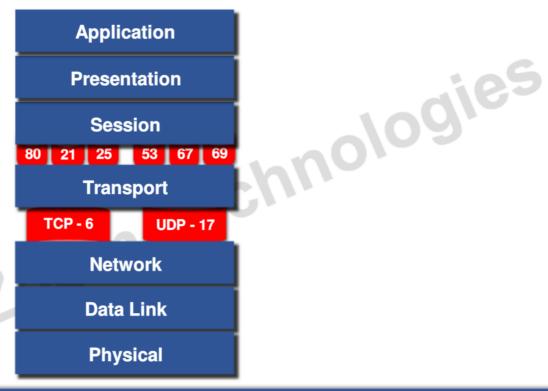
Reserved Ports

Open Ports 700M



Multiplexing & De-multiplexing







Transport Layer Protocols



• The protocols which takes care of Data Transportation at Transport layer are TCP and UDP

TCP UDP

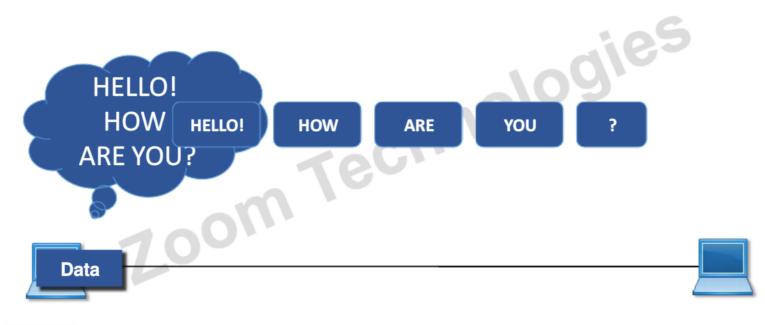
- Transmission Control Protocol
- Connection Oriented
- Supports Acknowledgements
- Reliable communication
- Slower data Transportation
- Protocol No is 6
- Ex: HTTP, FTP, SMTP

- User Datagram Protocol
- Connection Less
- No support for Acknowledgements
- Unreliable communication
- Faster data Transportation
- Protocol No is 17
- Ex: DNS, DHCP, TFTP



Segmentation









Sequencing



HELLO!





Sequencing



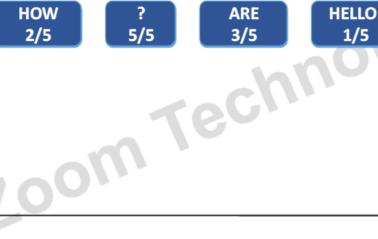
HELLO! YOU **HOW ARE** 3/5 4/5 1/5 2/5

om Data



Reassembling







ARE

HELLO!

YOU 4/5

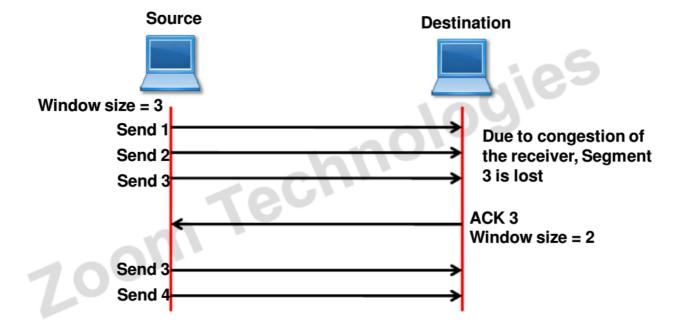






Flow Control and Error Correction



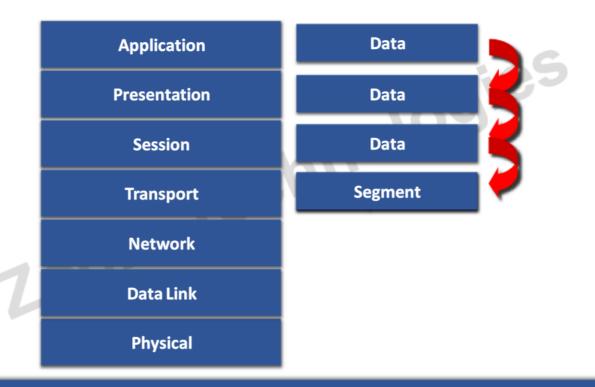






Data flow from Transport Layer







Network Layer



Application
Presentation
Session
Transport
Network
Data Link
Physical

Network Layer: It provides Logical addressing & Path determination (Routing)

The protocols that work in this layer are:

Routed Protocols:

IP, IPX, AppleTalk.. Etc

Routed protocols used to carry user data between hosts.

Routing Protocols:

RIP, OSPF.. Etc

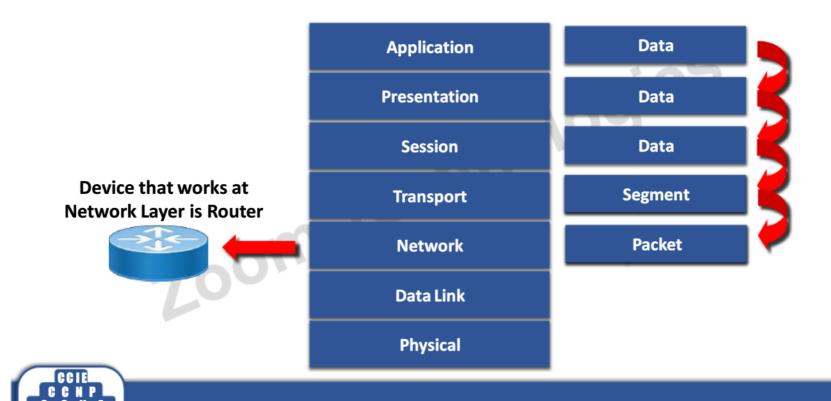
Routing protocols performs Path determination (Routing).





Data flow from Network Layer





Datalink Layer



Application	
Presentation	Ì
Session	Ì
Transport	
Network	
Data Link	
Physical	Ī

Datalink Layer

It has 2 sub layers

• MAC (Media Access Control) It provides reliable transit of data across a physical link.

It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check)

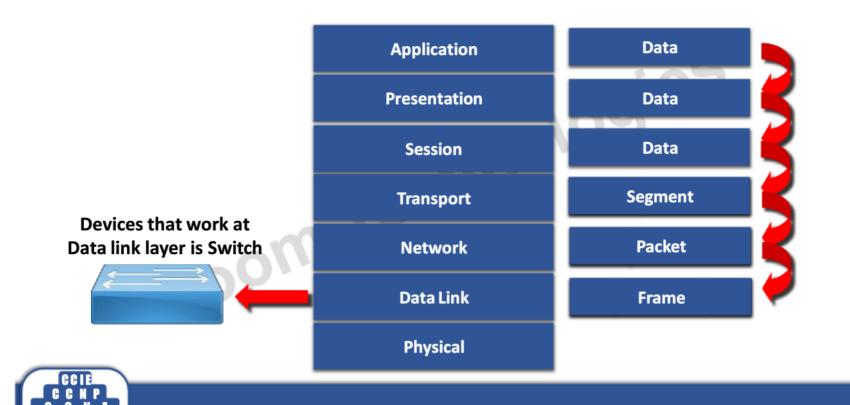
Ex: Ethernet, Token ring...etc

LLC (Logical Link Control)
 It provides communication with Network layer.



Data flow from Data link Layer





Physical Layer



Application
Presentation
Session
Transport
Network
Data Link
Physical

Physical Layer: It defines the electrical, Mechanical & functional specifications for communication between the Network devices.

The functions described at this layer are

Encoding/decoding:

It is the process of converting the binary data into signals based on the type of the media.

Copper media: Electrical signals of different voltages

Fiber media: Light pulses of different wavelengths

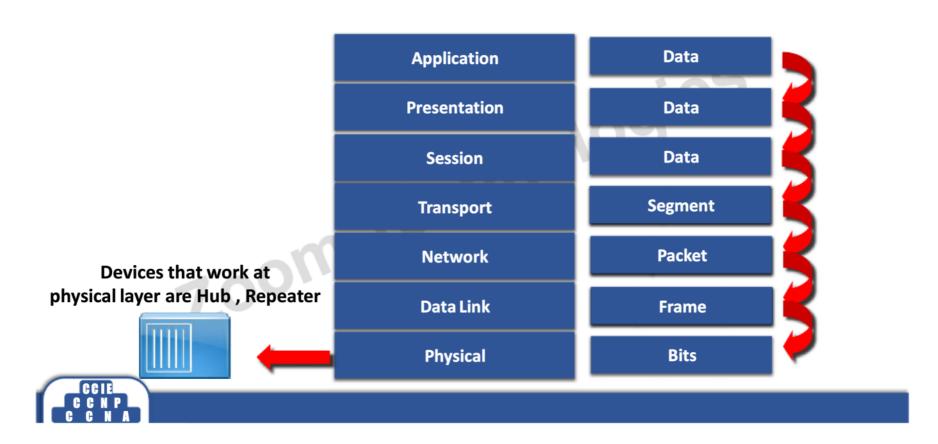
Wireless media: Radio frequency waves





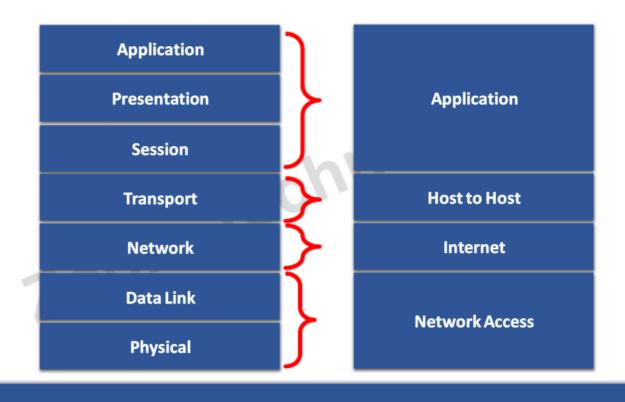
Data flow from Physical Layer

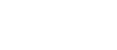


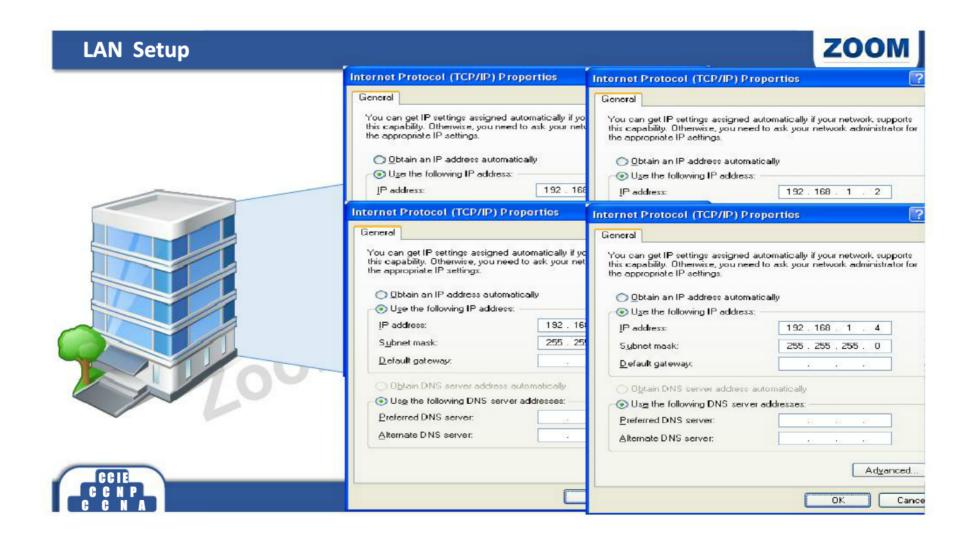


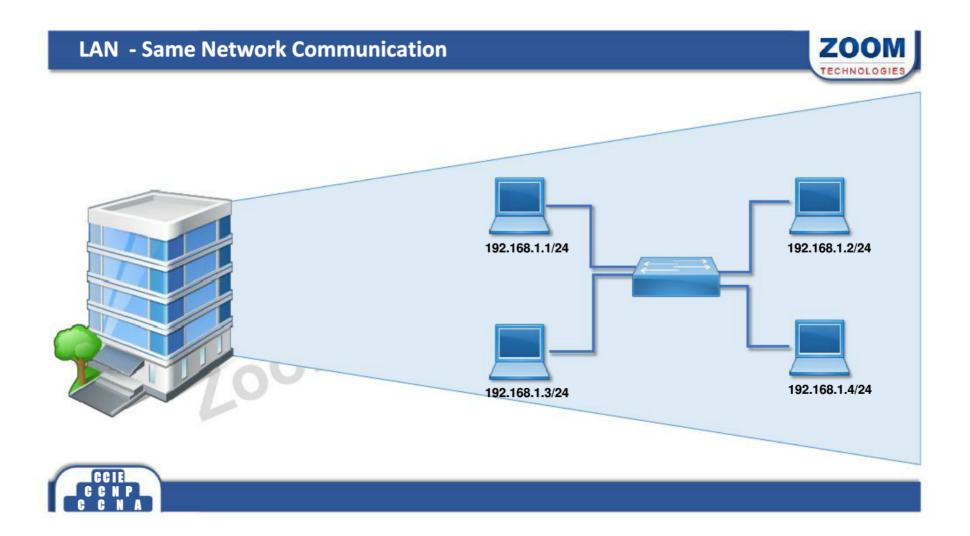
Comparison between OSI & TCP/IP Model















IP Address



- IP Address is a Logical Address
- Zoom Technologies • It is a Network Layer address (Layer 3)
- Two Versions of IP:
 - IP version 4 is a 32 bit address
 - IP version 6 is a 128 bit address





IP version 4



- Bit is represent by 0 or 1 (i.e. Binary)
- IP address in binary form (32 bits):
 01010101000001011011111100000001
- 32 bits are divided into 4 Octets:



• IP address in decimal form:

85.5.191.1



IPv4 address range



Taking Example for First Octet:

Total 8 bits, Value will be 0's and 1's

i.e. $2^8 = 256$ combination

1 1 1 1 1 1 1 1 = 255

Total IP Address Range
0.0.0.0
to
255.255.255.255



Binary to Decimal



128	64	32	16	8	4	2	1	Answer
1	1	0	0	0	0	0	0	192
0	0	0	0	1	0	1	0	10
1	0	1	0	1	0	0	0	168
1	0	1	0	1	1	0	0	172
0	0	0	1	0	0	0	0	16



Decimal to Binary



Decimal	128	64	32	16	8	4	2	1
18	0	0	0	1	0	0	1	0
152	1	0	0	1	1	0	0	0
200	1	1	0	0	1	0	0	0
15	0	0	0	0	1	1	1	1
240	1	1	1	1	0	0	0	0





IP Address Classification



IP address are divided into 5 Classes





Priority Bit



- Priority Bit is used for IP Address classification.
- Most significant bit(s) from the first octet are selected for Priority Bit(s). echnolog
- · Class A priority bit is 0
- Class B priority bits are 10
- · Class C priority bits are
- · Class D priority bits are 1110
- Class E priority bits are 1111



Class A Range



- In Class A: First bit of the first octet is reserved as priority bit, bit value is zero.
- Oxxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

Class A Range 0.0.0.0 to 127.255.255



Class B Range



- In Class B: First two bits of the first octet are reserved as priority bits, bit value as 10.
- 10xxxxxx. xxxxxxxxx. xxxxxxxxx

Class B Range 128.0.0.0 to 191.255.255



Class C Range



- In Class C: First three bits of the first octet are reserved as priority bits, bit value as 110.
- 110xxxxx. xxxxxxxxx. xxxxxxxxx

```
2<sup>7</sup> 2<sup>6</sup> 2<sup>5</sup> 2<sup>4</sup> 2<sup>3</sup> 2<sup>2</sup> 2<sup>1</sup> 2<sup>0</sup>

1 1 0 0 0 0 0 0 = 192

1 1 0 0 0 0 0 1 = 193

1 1 0 0 0 0 1 0 = 194

1 1 0 0 0 1 1 = 195

1 1 0 1 1 1 1 1 1 = 223
```

Class C Range 192.0.0.0 to 223.255.255



Class D Range



- In Class D: First four bits of the first octet are reserved as priority bits, bit value as 1110.
- 1110xxxx. xxxxxxxx. xxxxxxxx xxxxxxx

Class D Range 224.0.0.0 to 239.255.255





Class E Range



- In Class E: First four bits of the first octet are reserved as priority bits, bit value as 1111.
- 1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2⁷ 2⁶ 2⁵ 2⁴ 2³ 2² 2¹ 2⁰

1 1 1 1 0 0 0 0 = 240

1 1 1 1 0 0 0 1 = 241

1 1 1 1 0 0 1 0 = 242

1 1 1 1 1 0 1 0 0 = 244

1 1 1 1 1 1 1 1 1 1 1 1 1 = 255

Class E Range 240.0.0.0 to 255.255.255



Ranges



Class A Range 0.0.0.0 to 127.255.255.255 Class B Range 128.0.0.0 to 191.255.255.255 Class C Range 192.0.0.0 to 223.255.255.255

Class D Range 224.0.0.0 to 239.255.255.255

Class E Range 240 . 0 . 0 . 0 to 255 . 255 . 255 .255



Identifying Class



IP Address	Class
10.1.100.1	Α
150.17.2.200	В
192.1.1.1	С
224.0.0.10	D
120.200.1.1	Α



Octet Format



- IP address is divided into Network & Host Portion
 - CLASS A is written as
 N.H.H.H
 - CLASS B is written as N.N.H.H
 - CLASS C is written as N.N.N.H





1010gies

CLASS A - No. Networks & Hosts



Class A Octet Format is N.H.H.H

Network bits: 8 Host bits: 24

- No. of Networks
 - 2no of network bits-Priority bit
- achnologies (-1 is Priority Bit for Class A)
 - **2**⁷
 - 128 2 (-2 is for 0 & 127 Network) =
 - 126 Networks
- No. of Host
 - 2no of host bits -2
 - 2²⁴ 2 (-2 is for Network ID & Broadcast ID) =
 - 16777216 2
 - 16777214 Hosts/Network



CLASS B - No. Networks & Hosts



Class B Octet Format is N.N.H.H

Network bits: 16 Host bits: 16

- No. of Networks
 - 2 no of network bits-Priority bit
 - **2**¹⁶⁻² (-2 is Priority Bit for Class B)
 - **2**¹⁴
 - 16384 Networks =
- No. of Host
 - 2no of host bits -2
- echnologies 2¹⁶ – 2 (-2 is for Network ID & Broadcast ID) =
 - 65536 2 =
 - 65534 Hosts/Network



CLASS C - No. Networks & Hosts



Class C Octet Format is N.N.N.H

Network bits: 24 Host bits: 8

- No. of Networks
 - 2no of network bits-Priority bit
 - **2**²⁴⁻³ (-3 is Priority Bit for Class C)
 - **2**²¹
 - **2097152 Networks**
- No. of Host
 - 2no of host bits -2
- echnologie⁵ 28 – 2 (-2 is for Network ID & Broadcast ID) =
 - 256 2
 - 254 Hosts/Network



Network & Broadcast Address



- Network address: IP address with all bits as ZERO in the host portion.
- · Broadcast address: IP address with all bits as ONES in the host portion.
- · Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

Zoom





Example - Class A

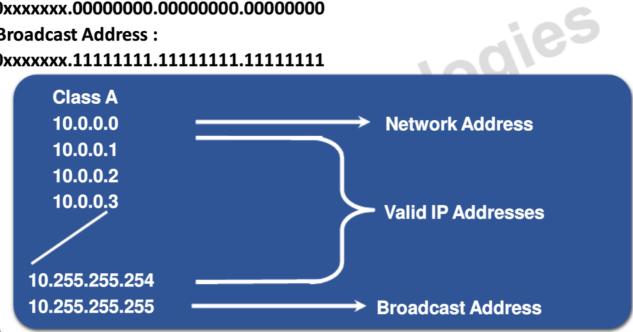


- Class A: N.H.H.H
 - Network Address:

0xxxxxx.00000000.0000000.00000000

- Broadcast Address:

0xxxxxx.11111111.11111111.11111111





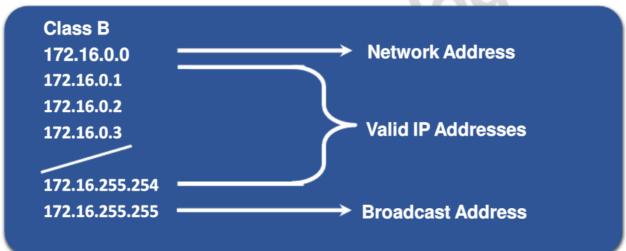
Example - Class B



- Class B: N.N.H.H
 - Network Address:

10xxxxxx.xxxxxxxx.00000000.00000000

- Broadcast Address:



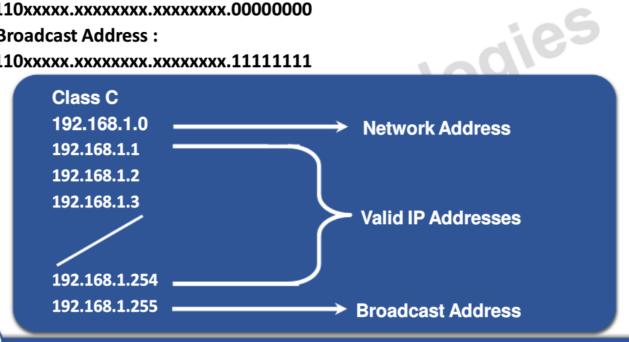




Example - Class C



- Class C: N.N.N.H
 - Network Address:
 - 110xxxxx.xxxxxxxxx.00000000
 - Broadcast Address :
 - 110xxxxx.xxxxxxxxxxxx.11111111





Identifying Network Address and Broadcast Address



IP Address	Network Address and Broadcast Address
120.1.1.1	120.0.0.0 and 120.255.255.255
172.16.1.1	172.16.0.0 and 172.16.255.255
10.100.1.10	10.0.0.0 and 10.255.255.255
192.168.1.10	192.168.1.0 and 192.168.1.255
150.10.1.1	150.10.0.0 and 150.10.255.255





Private IP Address



- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
- These addresses are not Routable (or) valid on Internet.

Class A 10.0.0.0 to 10.255.255.255

Class B 172.16.0.0 to 172.31.255.255

Class C 192.168.0.0 to 192.168.255.255



Subnet Mask



- Subnet Mask differentiates the Network and Host portions of an IP address
- Represented with all 1's in the network portion and with all 0's in the host portion.





Subnet Mask - Examples



ologies

Class A: N.H.H.H
 11111111.00000000.00000000.0000000
 Default Subnet Mask for Class A is 255.0.0.0



Default subnet mask



IP Address	Default subnet mask
17.1.1.1	255.0.0.0
202.1.0.18	255.255.255.0
190.10.1.1	255.255.0.0
102.10.1.10	255.0.0.0
192.0.0.1	255.255.255.0





How Subnet Mask Works?



ogies

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

ANDING PROCESS:

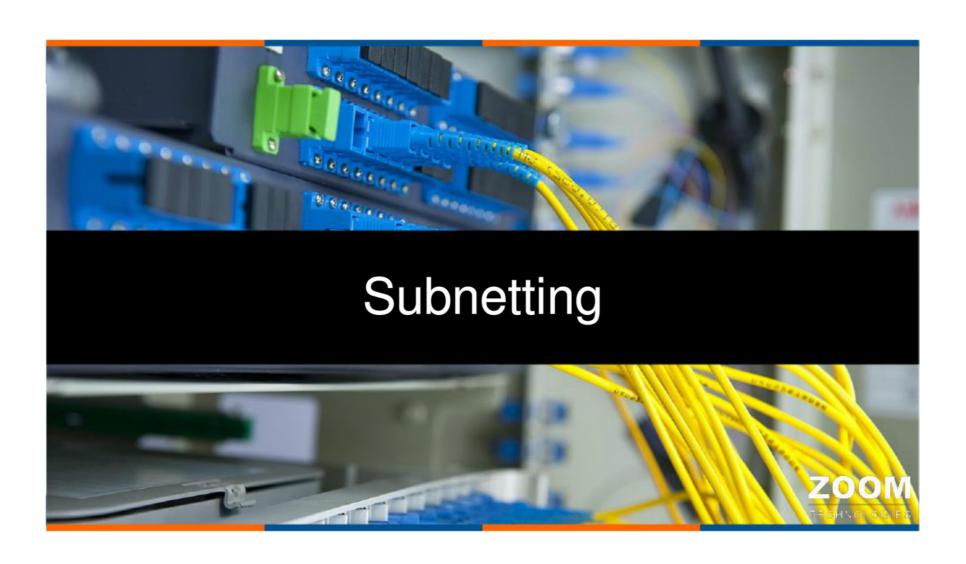
192.168.1.1 = **11000000.10101000.0000001.00000001**

192.168.1.0 = **11000000.10101000.00000001.00000000**

The output of an AND table is 1 if both its inputs are 1.

For all other possible inputs the output is 0.





Subnetting



- Creating Multiple independent Networks from a single Network
- Converting Host bits into Network bits (i.e. converting 0's into 1's)
- Subnetting can be performed in two ways
- FLSM (Fixed Length Subnet Mask)
- VLSM (Variable Length Subnet Mask)
- Subnetting can be done based on requirement
- Number of Networks Required?
- Number of Hosts Required?

Note:- It is very Useful for Internet Service Providers (ISP), Large Organizations /Companies etc.,

ologies



Requirement of Networks



- A corporate network has 200 PC's
- Which class of IP Address is preferred for the network? ologies

Answer: class C

There are 4 departments with 50 pc's each

Marketing = 192.168.1.1 to 192.168.1.50 **Sales** 192.168.1.51 to 192.168.1.100 **Finance** 192.168.1.101 to 192.168.1.150 IT 192.168.1.151 to 192.168.1.200







- · Administrators requirement :
- Inter-department communication should not be there

Solution:

hnologies Allocate different Networks to each Department

i.e.,

192.168.1.1 to 192.168.1.50 Sales 192.168.2.1 to 192.168.2.50 192.168.3.1 to 192.168.3.50 **Finance** IT 192.168.4.1 to 192.168.4.50



Main Aim of Subnetting



- · Problem with the previous scenario is
- Zoom Technologies Wastage of IP addresses, if it is Public IP addresses (Approx. 800)
- · To reduce the wastage of IP addresses, we have Subnetting
- Requirement of Networks





Requirement of Subnets – 4 no's?



Class C: 192.168.1.0

255.255.255.0

Subnets required: 4 no's

 $= 2^n \ge \text{Req. of Subnet}$

 $= 2^n \ge 4$

 $= 2^2 \ge 4$

= 4 subnets

Customized subnet mask =

255.

255.

255.

echnologie⁵

1111111. 11111111. 11111111. 00000000

. 11000000

255.

255.

255.

192





alogies

Calculation of Hosts / subnet

- = 2h 2 (-2 is for Network ID & Broadcast ID)
- $= 2^6 2$
- = 64 2
- = 62 Hosts/subnet

Subnet Range

Network ID Broadcast ID

192.168.1.1 to 192.168.1.63 192.168.1.64 to 192.168.1.127

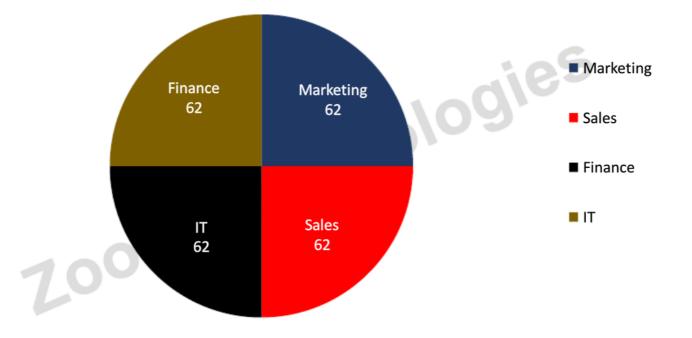
192.168.1.128 to 192.168.1.191

192.168.1.192 to 192.168.1.255



FLSM







VLSM



- Subnetting a subnet is called as Variable Length Subnet Mask
- VLSMs provide the capability to include more than one subnet mask within a major network



Requirement of Hosts



· In corporate network there are 4 departments and their requirement as follows,

Marketing -10

Sales 50

Finance 25

IT 100

echnologies Arrange them in Descending Order

100 IT

Sales 50

25 **Finance**

Marketing • 10



Requirement of Hosts



Class C: 192.168.1.0

255.255.255.0

echnologie⁵ Hosts required: 100, 50, 25 and 10

First, we calculate for IT = 100 Hosts

 $2^h - 2 \ge \text{Req. of Hosts}$

 $= 2^{h} - 2 \ge 100$

 $= 2^7 - 2 \ge 100$

= 128 - 2 = 126 hosts/subnet

Customized subnet mask =

255. 255. 255. 11111111. 11111111. 11111111. 00000000

. 10000000

255. 255. **255.** 128





Calculation of subnets

- = 2ⁿ
- $= 2^1$
- = 2
- = 2 Hosts/subnet

Subnet Range

Network ID Broadcast ID

192.168.1.0 to 192.168.1.127 | | 192.168.1.128 to 192.168.1.255

hnologies





Now, Available network is 192.168.1.128 to 192.168.1.255

Next, we calculate for Sales = 50 Hosts

$$2^h - 2 \ge \text{Req. of Hosts}$$

$$= 2^{h} - 2 \ge 50$$

$$= 2^6 - 2 \ge 50$$

$$= 64 - 2 = 62 \text{ hosts/subnet}$$

Customized subnet mask =

echnologie⁵ 128 255. 255. 255.

11111111. 11111111. 11111111. 10000000

. 11000000

255. 255. 255. 192





Calculation of subnets

- = 2ⁿ
- $= 2^1$
- = 2
- = 2 Hosts/subnet

Subnet Range

Network ID Broadcast ID

192.168.1.128 to 192.168.1.191 > SALES 192.168.1.192 to 192.168.1.255

hnologies





• Similarly, we can calculate for Finance = 25 Hosts

Using 192.168.1.192 to 192.168.1.255 echnologies

Subnet Mask 255.255.255.192

$$2^h - 2 \ge \text{Reg. of Hosts}$$

- $= 2^{h} 2 \ge 25$
- $= 2^5 2 \ge 25$
- = 32 2 = 30 hosts/subnet

Customized subnet mask =

255. 255. 255. 192

11111111. 11111111. 11111111. 11000000

. 11100000

255. 224 **255. 255.**





Subnet Range

Network ID Broadcast ID

192.168.1.192 to 192.168.1.223 **FINANCE** 192.168.1.224 to 192.168.1.255

• For Marketing = 10 Hosts

Using 192.168.1.224 to 192.168.1.255 with Subnetmask 255.255.255.224

 If we calculate, then we will get customized subnet mask 255.255.255.240 and Range as follows

Subnet Range

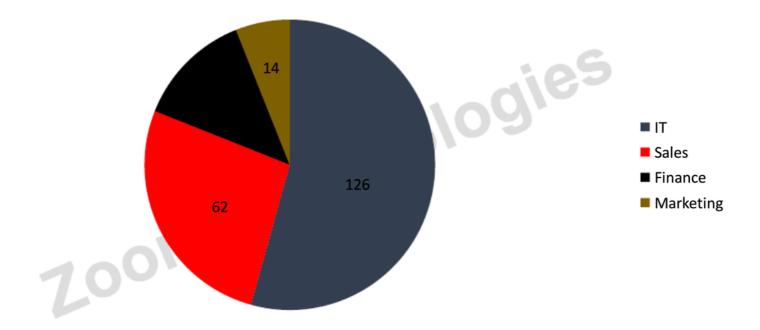
Network ID Broadcast ID

192.168.1.224 to 192.168.1.239 **MARKETING** 192.168.1.240 to 192.168.1.255



VLSM









Power table



PO			

		TOWEIT TABLE	
21 = 2	29 = 512	2 ¹⁷ = 131072	2 ²⁵ = 33554432
$2^2 = 4$	2 ¹⁰ = 1024	2 ¹⁸ = 262144	2 ²⁶ = 67108864
23 = 8	211 = 2048	2 ¹⁹ = 524288	2 ²⁷ = 134217728
24 = 16	212 = 4096	2 ²⁰ = 1048576	2 ²⁸ = 268435456
25 = 32	213 = 8192	2 ²¹ = 2097152	2 ²⁹ = 536870912
2 ⁶ = 64	214 = 16384	2 ²² = 4194304	2 ³⁰ = 1073741824
2 ⁷ = 128	2 ¹⁵ = 32768	2 ²³ = 8388608	2 ³¹ = 2147483648
28 = 256	2 ¹⁶ = 65536	2 ²⁴ = 16777216	2 ³² = 4294967296



Some Important Values



VALUES IN SUBNET MASK				
Bit	Value	Mask		
1	128	10000000		
2	192	11000000		
3	224	11100000		
4	240	11110000		
5	248	11111000		
6	252	11111100		
7	254	11111110		
8	255	11111111		





Example – 1: Requirement of subnet is 14?



Class C: 192.168.1.0

Requirement of Subnet

 $2^n \ge \text{Req. of Subnet}$

=

No. of Hosts/subnet

Thosts/subnet

2h-2 (-2 is for Network ID & Broadcast ID)

24-2

16-2

14 Hosts/Subnet



Example – 1 (Continued...)



Customized Subnet Mask =



Range of Networks

Network ID	Broadcast ID
192.168.1.0	192.168.1.15
192.168.1.16	192.168.1.31
192.168.1.32	192.168.1.47
192.168.1.48	192.168.1.63

192.168.1.224	192.168.1.239
192.168.1.240	192.168.1.255



Example - 1 (Continued...)



If you convert 4 Host Bits to Network Bits 16 Subnet & 14 Hosts/Subnet

> **Customized Subnet Mask** 255.255.255.240

> > **Subnet Range**

192.168.1.16 to 192.168.1.31 192.168.1.32 to 192.168.1.47 192.168.1.48 to 192.168.1.63 192.168.1.64 to 192.168.1.79

192.168.1.224 to 192.168.1.239 192.168.1.240 to 192.168.1.255



Example - 2: Requirement of Hosts is 2?



Class C: 192.168.1.0 **Requirement of Host**

 $2^h - 2 \ge \text{Req. of Host}$

ubnet $2^2 - 2 \ge 2$ (-2 is for Network ID & Broadcast ID)

2 Hosts/Subnet

No. of Subnets

2ⁿ

26

64 =

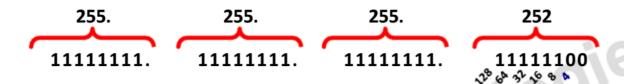
64 Subnet



Example - 2 (Continued...)



Customized Subnet Mask =



Range of Networks

Network ID	Broadcast ID
192.168.1.0	192.168.1.3
192.168.1.4	192.168.1.7
192.168.1.8	192.168.1.11
192.168.1.12	192.168.1.15

192.168.1.248	192.168.1.251
192.168.1.252	192.168.1.255



Example - 3: Requirement of Networks is 4?



Class B: 172.16.0.0 **Requirement of Subnet**

 $2^n \ge \text{Req. of Subnet}$

No. of Host

Host 2^h – 2 (-2 is for Network ID & Broadcast ID) 2¹⁴ – 2 16384 – 2 16382 Hosts/Sub-

=

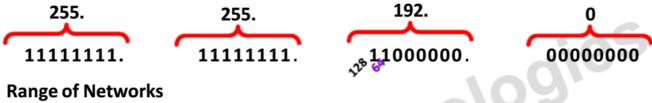
=



Example – 3 (Continued...)



Customized Subnet Mask =



Network ID	Broadcast ID
172.16.0.0	172.16.63.255
172.16.64.0	172.16.127.255
172.16.128.0	172.16.191.255
172.16.192.0	172.16.255.255



Example – 4: Requirement of Hosts is 126?



Class B: 172.16.0.0 **Requirement of Hosts**

 $2^h - 2 \ge \text{Req. of Host}$

m Technologies $2^7 - 2 \ge 126$ (-2 is for Network ID & Broadcast ID)

128 - 2

126 Hosts/Subnet

No. of Subnets

2ⁿ =

29

512 =

512 Subnets =



Example – 4 (Continued...)



Customized Subnet Mask =

255.	255.	255.	128
11111111.	11111111.	11111111.	10000000
Range of Network	ks		31001
Netwo	rk ID	Broadcast	ID
172.16	.0.0	172.16.0.1	127
172.16	.0.128	172.16.0.2	255
172.16	.1.0	172.16.1.1	127
172.16	.1.128	172.16.1.2	255
	O_{III}		
7.0			
172.16	.255.0	172.16.25	5.127
	.255.128	172.16.25	5.255



Scenario



A co-operate network is having 100 PC

Co-operate - 192.168.1.0/24

- Marketing
- Sales
- Accounts
- H/R
- Training

echnologies er-de Administrator's requirement: Inter-department communication should not be possible?

Best Solution is:

FLSM i.e. Subnetting



Scenario (...continued) ZOOM TECHNOLOGIES **CO-OPERATE NETWORK** Now we are also having sub departments **I MARKETING SALES** - Purchase - Stock 7.00m Techno **ACCOUNTS** Billing Salary Loans Stationary Tax Interview **Public relation**

Scenario (...continued)



Finance

Administrator does not want inter-department communication in the sub departments?

..aller ran Answer: You will use the subnet range to further divide it into smaller ranges, this time its Subnetting of a Subnet i.e. VLSM.





Calculation of FLSM



Class C: 192.168.1.0 **Requirement of Subnet**

 $2^n \ge \text{Req. of Subnet}$

 $2^3 \geq 5$

= 8

8 Subnet

No. of Hosts/subnet

ologies 2^h – 2 (-2 is for Network ID & Broadcast ID)

 $2^5 - 2$

32 – 2

30 Hosts/Subnet



(Continued...)



Customized Subnet Mask =

255.	255.	255.	224
11111111.	11111111.	11111111.	11100000 \$\$ \$\ship\$
Range of Networ	ks		7/02
Netw	ork ID	Broadcas	t ID
192.16	58.1.0	192.168.1	.31

Range of Networks

Broadcast ID
192.168.1.31
192.168.1.63
192.168.1.95
192.168.1.127
192.168.1.159
192.168.1.191
192.168.1.223
192.168.1.255



Assigning of the Ranges



CO-OPRATE NETWORK

```
MARKETING
                    → 192.168.1.32 − 1.63/27
                              echnologies
SALES
                      192.168.1.64 - 1.95/27
   Purchase
   └ Stock
 ACCOUNTS
                    → 192.168.1.96 − 1.127/27
   Billing
   - Salary
   - Loans
    - Stationary
   ∟ Tax
                      192.168.1.128 - 1.159/27
H/R
   Interview
     Public relation
   └ Finance
I TRAINING
                     > 192.168.1.160 – 1.191/27
```



Calculation of VLSM for CISCO Dept.



Class C: 192.168.1.64 **Requirement of Subnet**

 $2^n \ge \text{Req. of Subnet}$

=

No. of Host

Host

2h – 2 (-2 is for Network ID & Broadcast ID)

2⁴ – 2

16 – 2

14 Hosts/Subpose

=

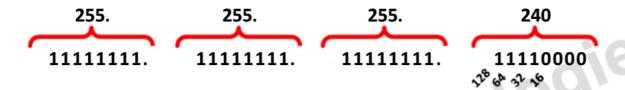
=



VLSM (Continued...)



Customized Subnet Mask =



Range of Networks

 Network ID
 Broadcast ID

 192.168.1.64
 192.168.1.79

 192.168.1.80
 192.168.1.95



Assigning of the Ranges

FRAINING



CO-OPERATE NETWORK 192.168.1.32 – 1.63/27 MARKETING chnologies **SALES 192.168.1.64 – 1.95/27 192.168.1.64 – 1.79/28** Purchase 192.168.1.80 - 1.95/28 – Stock 192.168.1.96 - 1.127/27 **ACCOUNTS** - Billing - Salary - Loans └ Stationary - Tax **192.168.1.128 – 1.159/27** Interview **Public Relation** 192.168.1.160 – 1.191/27 - Finance

Calculation of VLSM for Firewall Dept.



Class C: 192.168.1.96 **Requirement of Subnet**

 $2^n \ge \text{Req. of Subnet}$

 $2^3 \ge 5$

8 Subnet

No. of Host

nologies 2^h – 2 (-2 is for Network ID & Broadcast ID)

 $2^2 - 2$ =

4 – 2

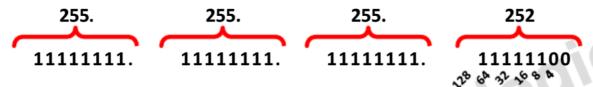
2 Hosts/Subnet



VLSM (Continued...)



Customized Subnet Mask =



Range of Networks

Network ID	Broadcast ID
192.168.1.96	192.168.1.99
192.168.1.100	192.168.1.103
192.168.1.104	192.168.1.107
192.168.1.108	192.168.1.111
192.168.1.112	192.168.1.115
192.168.1.116	192.168.1.119
192.168.1.120	192.168.1.123
192.168.1.124	192.168.1.127



Assigning of the Ranges



Nogies

```
CO-OPERATE NETWORK
                      192.168.1.32 – 1.63/27
    MARKETING
                        • 192.168.1.64 – 1.95/27
    SALES
                          192.168.1.64 - 1.79/28
      ├ Purchase
                       - Stock
                        ▶ 192.168.1.96 − 1.127/27
    ACCOUNTS
                        → 192.168.1.96 − 1.99/30
       Billing
                       192.168.1.100 - 1.103/30
       - Salary
                       192.168.1.104 – 1.107/30
       - Loans
                       192.168.1.108 – 1.111/30
       Stationary
                       192.168.1.112 – 1.115/30
      - Tax
                        192.168.1.128 – 1.159/27
    H/R
        Interview
       - Public Relation
                        → 192.168.1.160 – 1.191/27
      Finance
 TRAINING
```

Calculation of VLSM for Solaris Dept.



Class C: 192.168.1.128 **Requirement of Subnet** $2^n \ge \text{Req. of Subnet}$ =

No. of Host

Host

2h – 2 (-2 is for Network ID & Broadcast ID)

2³ – 2

8 – 2

6 Hosts/Subpet

= =

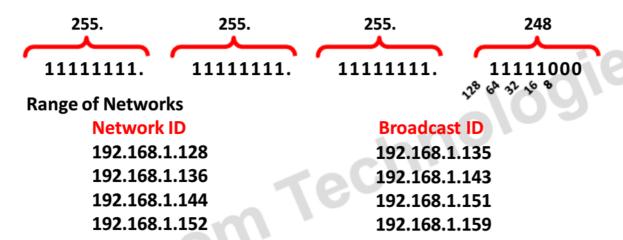




VLSM (Continued...)



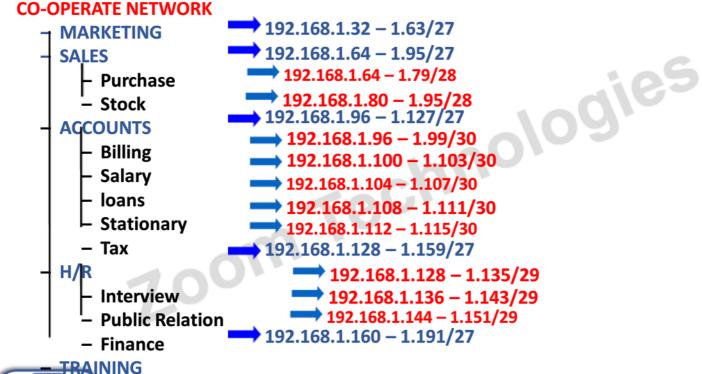
Customized Subnet Mask =





Assigning of the Ranges

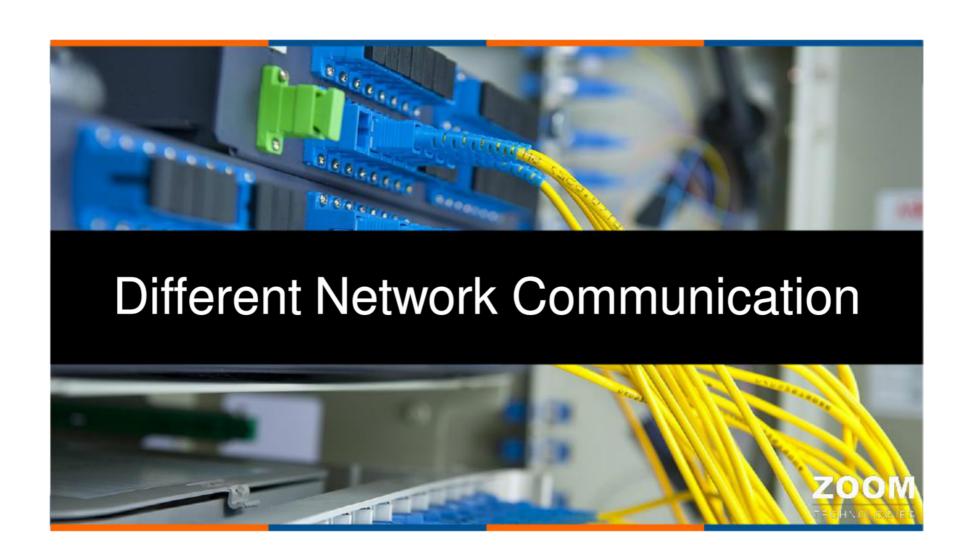






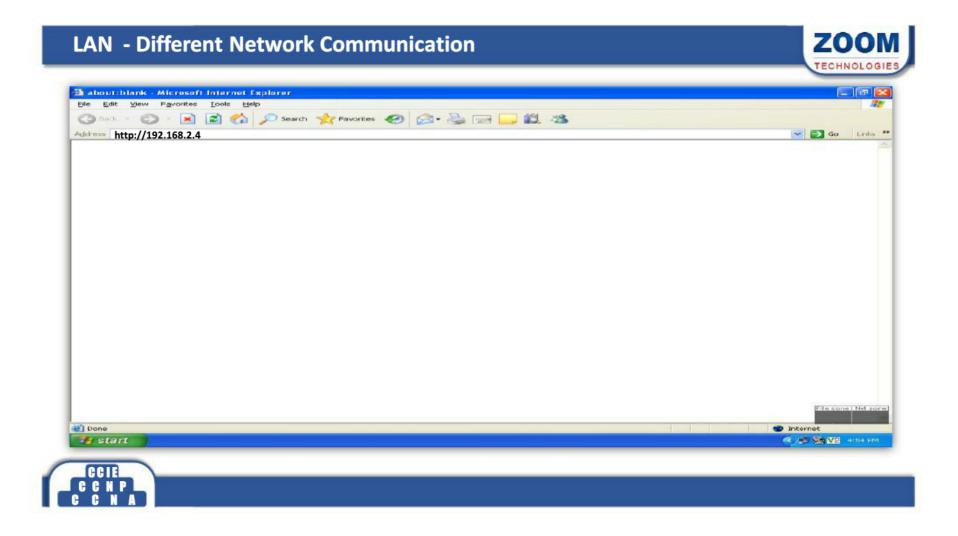
Slash notation	subnet mask
/8	255.0.0.0
/12	255.240.0.0
/16	255.255.0.0
/22	255.255.252.0
/24	255.255.255.0



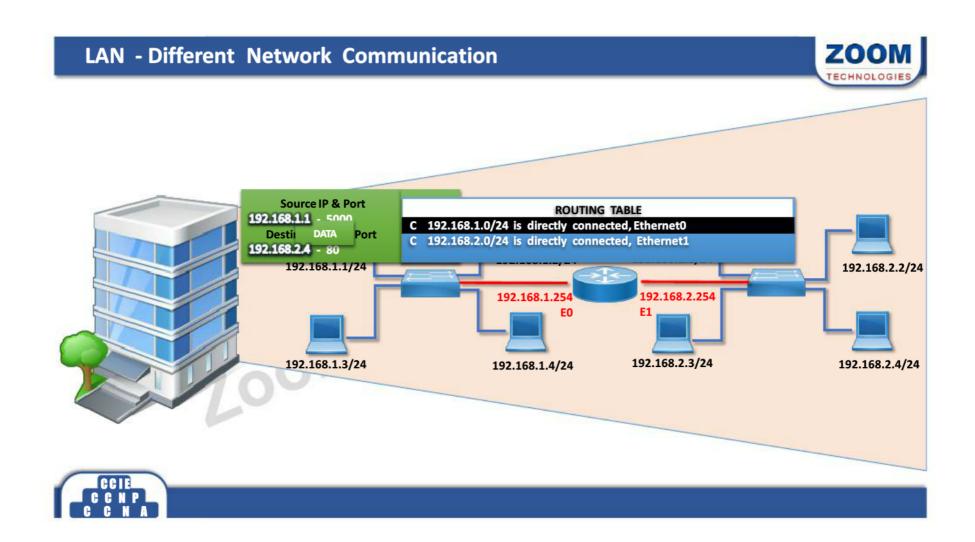


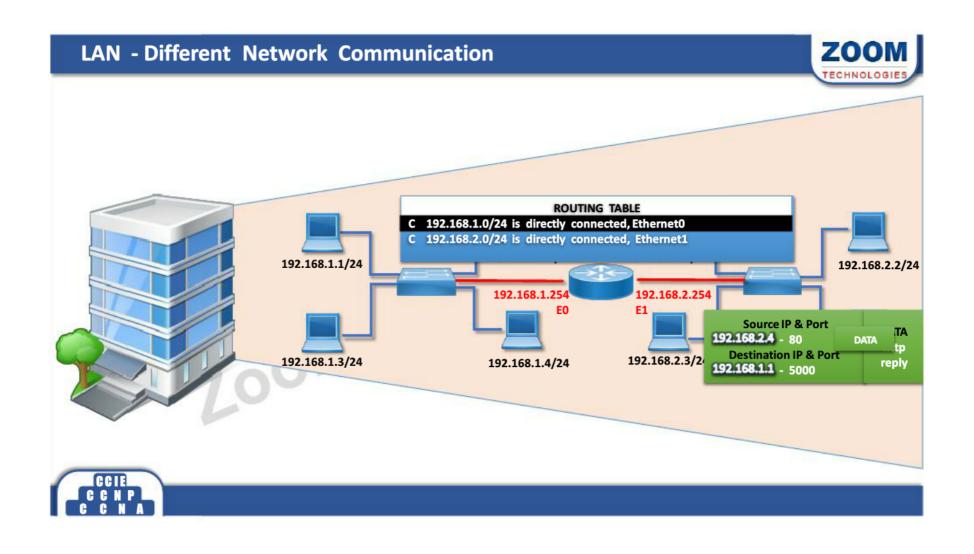


192.168.1.1/24 192.168.1.2/24 192.168.2.2/24 192.168.2.2/24 192.168.2.2/24 192.168.2.2/24 192.168.2.2/24 192.168.2.2/24





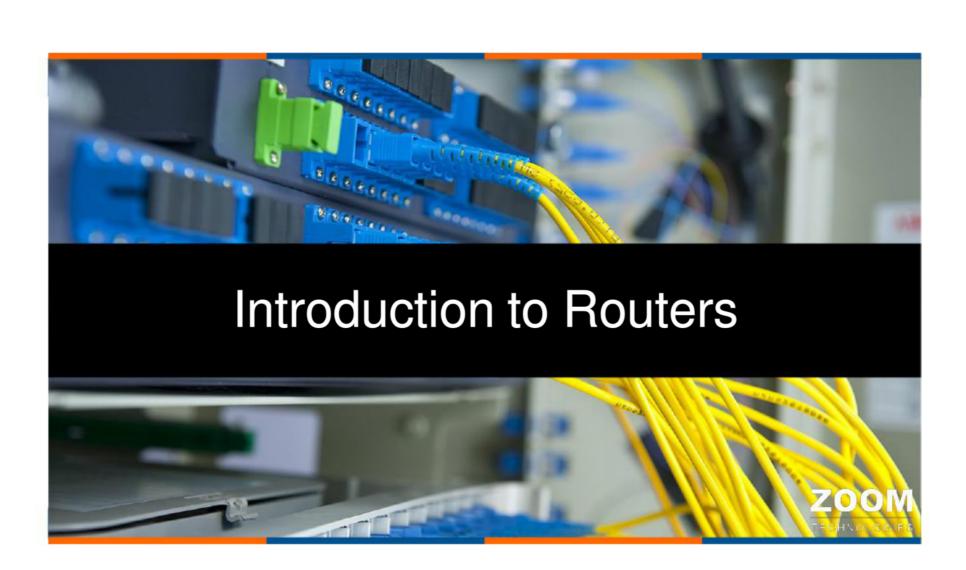




LAN - Different Network Communication









Router



- · Router is an internetworking device.
- It enables communication between two or more different logical networks.
- It is a Network Layer (layer 3) device.
- It comes from the word "ROUTE". Hence it is also a device that finds the best route (path) for networks.
- .ur all d€ The IP of Router is the default gateway for all devices in LAN.



Type of Routers

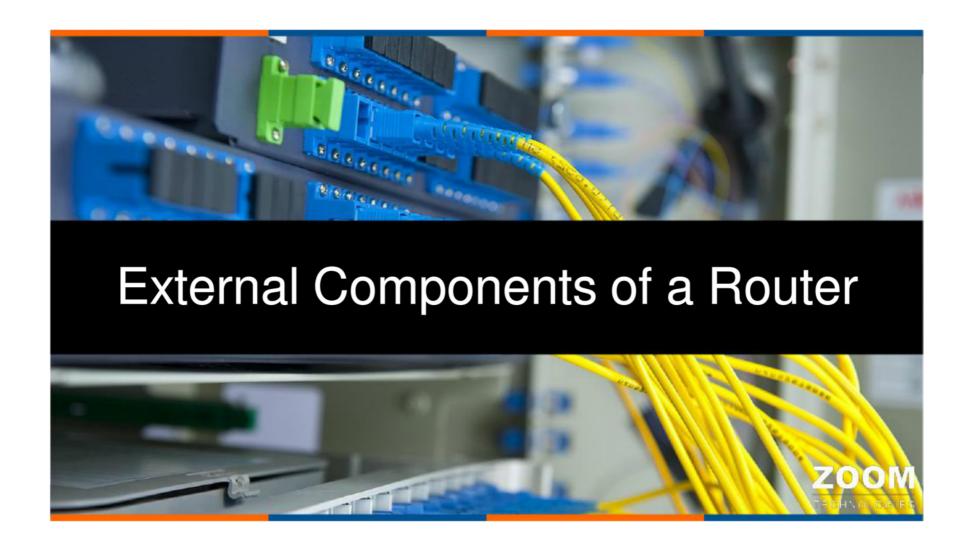


There are two type of Routers

- Hardware Routers:
- Zoom Technologies - Cisco, Juniper, Multicom, HP, Dlink, Maipu and many more...
- Software Routers:
 - Microsoft Server, Linux Server



Functions of a Router Inter-network Communication **Best Path Selection** 50/0/1 SO/0/0 **Packet Switching** · Packet forwarding S0/1 S0/0 S0/0 S0/1 F0/0 E0/0 Source IP & Port DATA DATA 191.0.0.10 - 80 61.0.0.1 http reply http **Destination IP & Port** Destination request 61.0.0.10 - 3000 191.0.0.10 - 80 Internet User www.yahoo.com 61.0.0.10 191.0.0.10



Hardware Routers



- Fixed Router
- Modular Router

Zoom Technologies



Fixed Router









Modular Router







2800 Series







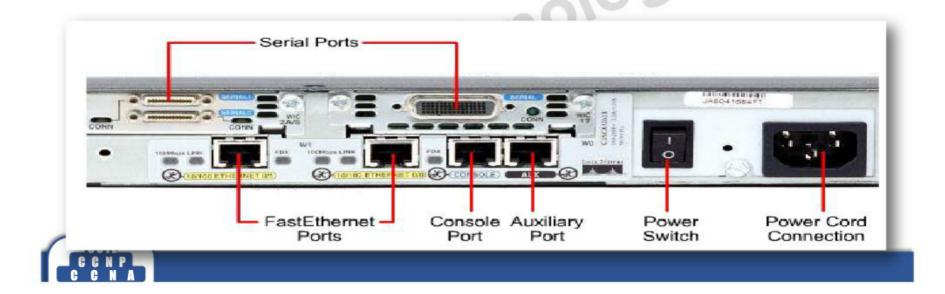




Types of routers







Attachment Unit Interface



- Attachment Unit Interface (AUI) is used to connect the Router to the LAN.
- It is also called as the Ethernet interface.
- AUI is an DB 15 pin female interface.
- Transceiver is used to connect AUI port to LAN HUB / Switch.
- Transceiver converts DB-15 signal to RJ-45.



Transceiver







Other LAN Interfaces - RJ-45 ports



- Routers have RJ-45 ports to connect the Router to the LAN.
- The speed of the RJ-45 ports can be
 - 10 Mbps Ethernet
 - 10/100 Mbps Fast Ethernet
 - Zoom Technologi - 10/100/1000 Mbps Gigabit Ethernet

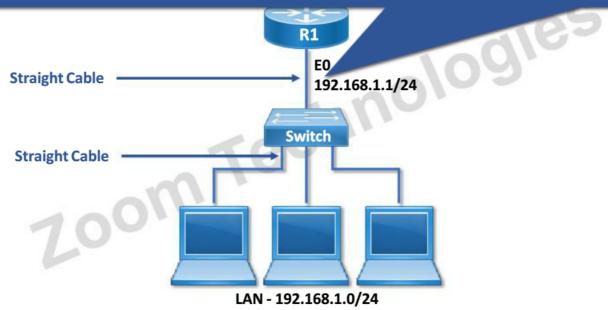




LAN Connectivity



An IP address has to be assigned to this interface. It should be in the same network as that of the LAN. This IP address is the default gateway address for all LAN systems.

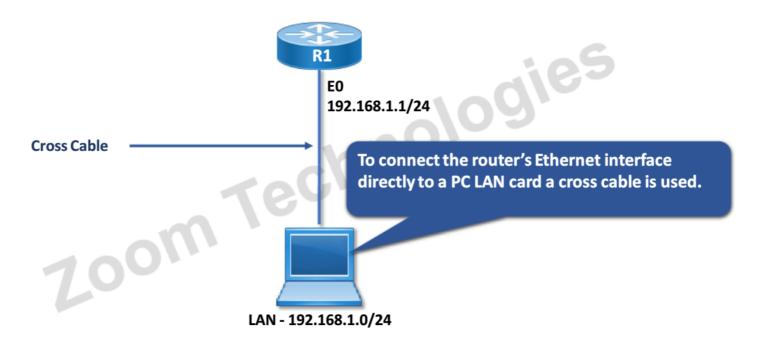






LAN Connectivity







Serial Port



- · Serial port is used for WAN Connectivity.
- Serial port are available as
 - 60 pin female connectors.
 - Smart Serial 26 pin female connectors.











HWIC



• High-speed WAN interface cards (HWICs) provide connectivity to a Wide Area Network





Console Port



- It is a local administrative port.
- It is a RJ-45 Port.
- It is used for initial configuration and advance troubleshooting.
- Note: It is the most important and sensitive port on the Router.



DB-9 Convertor



Console cable

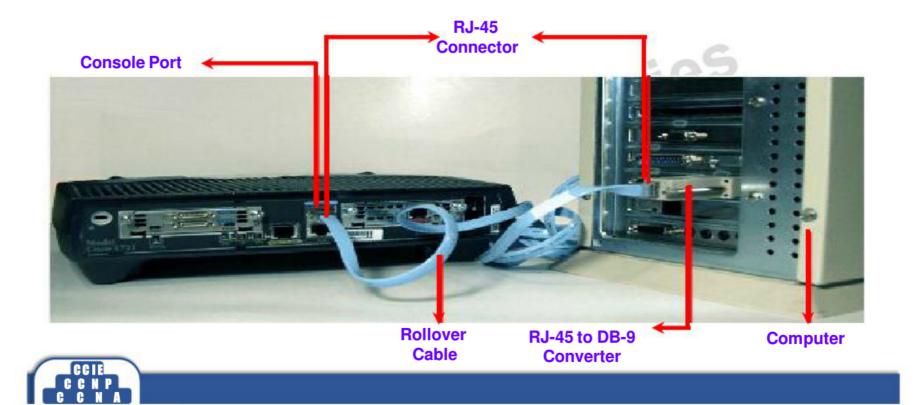






Console Connectivity





Auxiliary Port



- It is a remote administrative port.
- Used for remote administration / configuration.
- Its an RJ-45 port.
- A console / rollover cable is used to connect the auxiliary port to a dial-up modem.





Roll over Cable

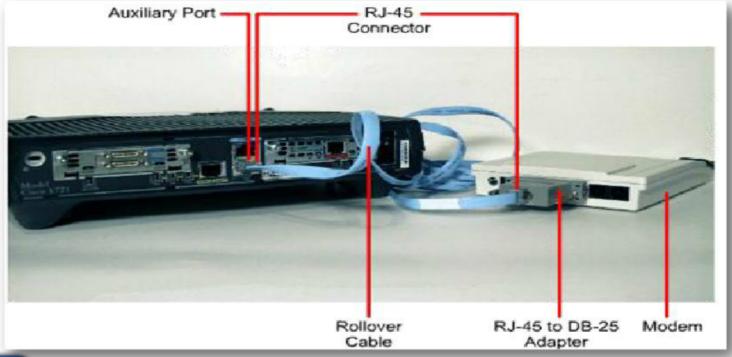


One End	Other End
Orange-white	Brown
Orange	Brown-white
Green-white	Green
Blue	Blue-white
Blue-white	Blue
Green	Green-white
Brown-white	Orange
Brown	Orange-white
Brown	



Auxiliary Connectivity







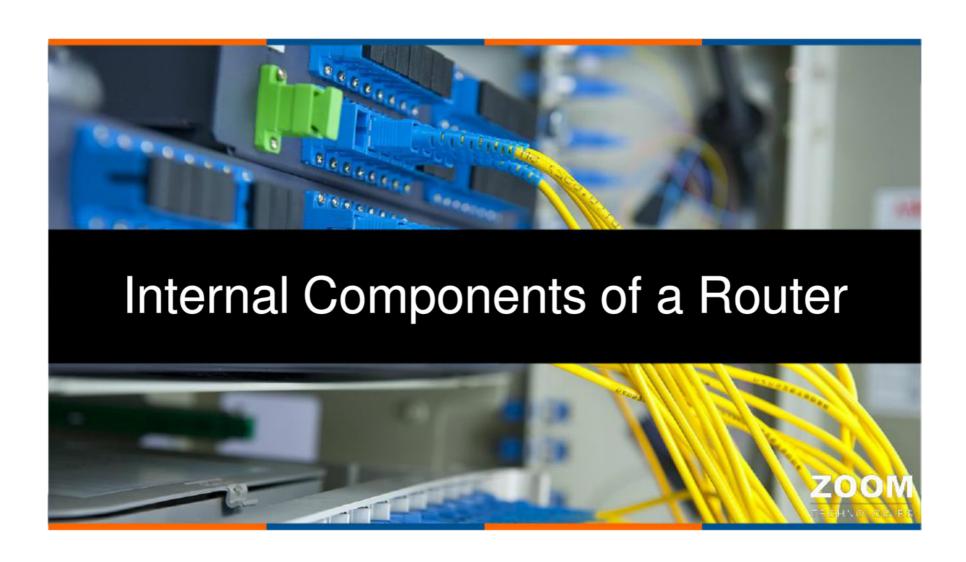


Interfaces of a Router



- LAN Interface
 - Attachment Unit Interface (AUI) 10 Mbps
 - Zoom Technologies - RJ 45 Ethernet / FastEthernet / GigabitEthernet
- WAN Interface
 - Normal Serial Interface
 - Smart Serial Interface
- Administrative Interface
 - Console
 - Auxiliary







Internal Components of Router



- ROM (Read only Memory)
 - It contains a bootstrap program which searches and loads the operating system.
 - It is similar to the BIOS of a PC.
 - It also contains a ROMMON for advance troubleshooting.
- · Flash memory
 - The Internetwork Operating System (IOS) is stored here.
 - IOS is a Cisco proprietary operating system.

7.00m



Internal Components of Router



- NVRAM (Non Volatile Random Access Memory)
 - NVRAM is similar to a hard disk.
 - It is also known as permanent storage.
 - The startup configuration is stored here.
- RAM (Random Access Memory)
 - It is also called as the main memory.
 - It is a temporary storage.
 - The running configuration is stored here.

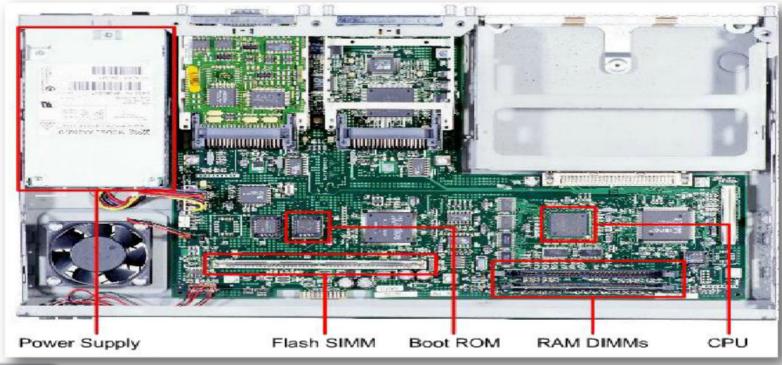




nologies

Internal Components of Router







BOOT Sequence



Power On Self Test – checks the hardware

ROM loads Bootstrap program and searches for the IOS

IOS from Flash is loaded

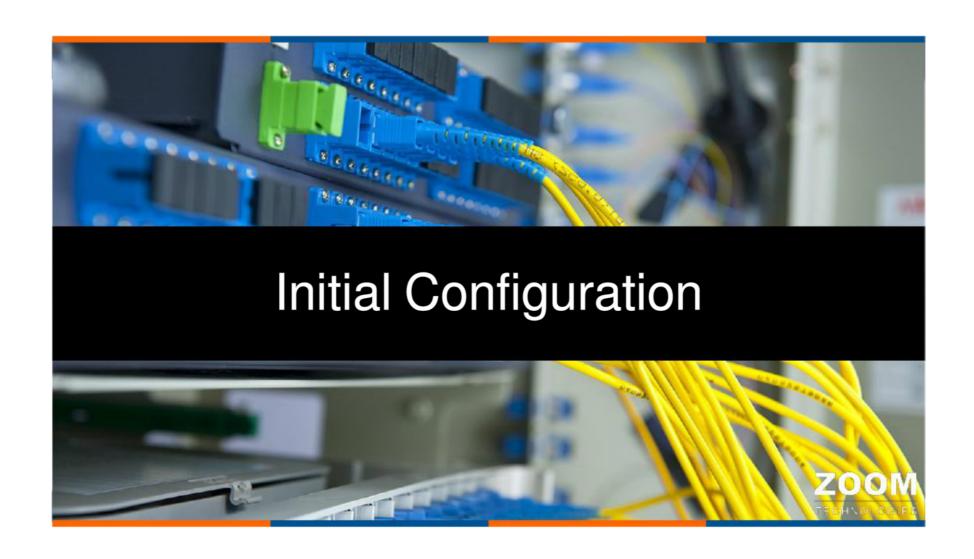
FLASH

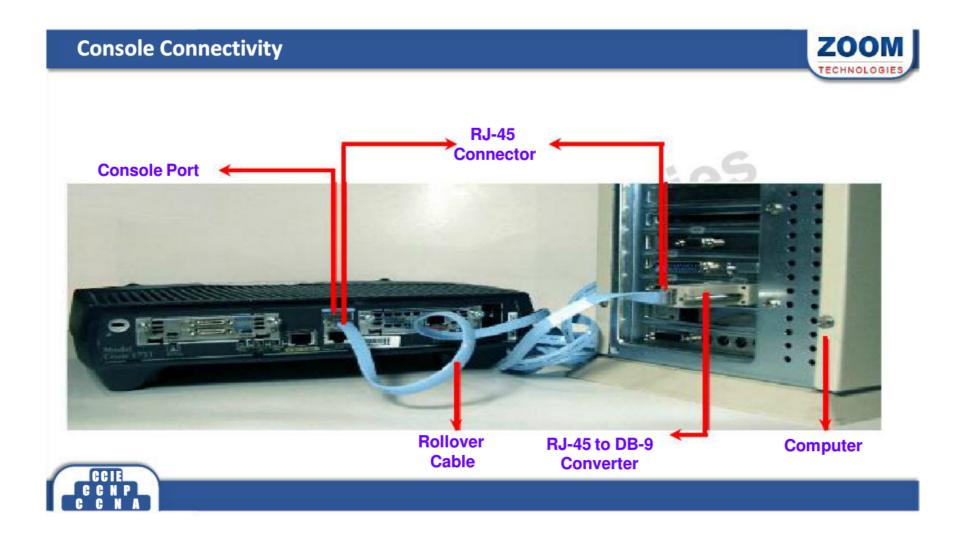
The startup configuration is loaded from the NVRAM

Boot process is completed as everything is loaded into the RAM









Console Connectivity



- · Cisco Routers & Switches does not have any default IP address or Configuration, hence require to use the Console port for Initial Configuration.
- Require physical connection between the Cisco Router/Switch and PC via console cable.







Emulation Software



WINDOWS

Zoom Technologies Hyper-terminal / Putty / Teraterm

LINUX

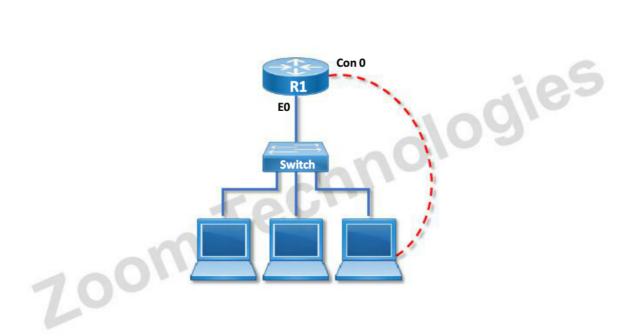
· Minicom -s





Initial Configuration

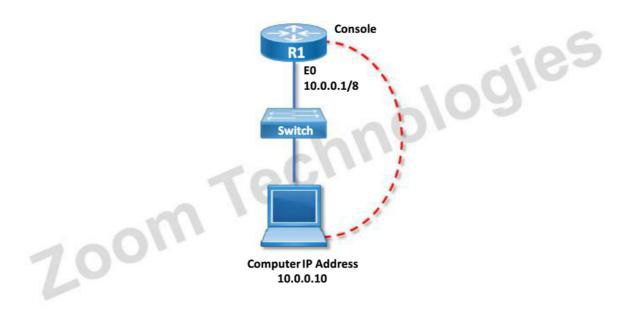






Accessing Router



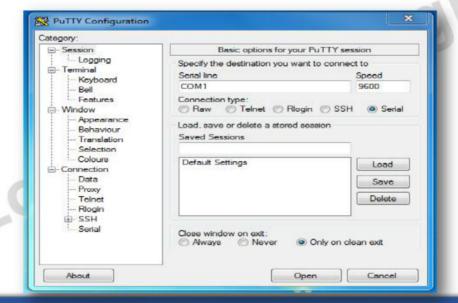








- · Accessing router via console from Microsoft Windows Computer
- Start a terminal emulator application, such as PUTTY.exe
- Select Serial option and set speed to 9600
- Click Open







Types of WAN Technologies

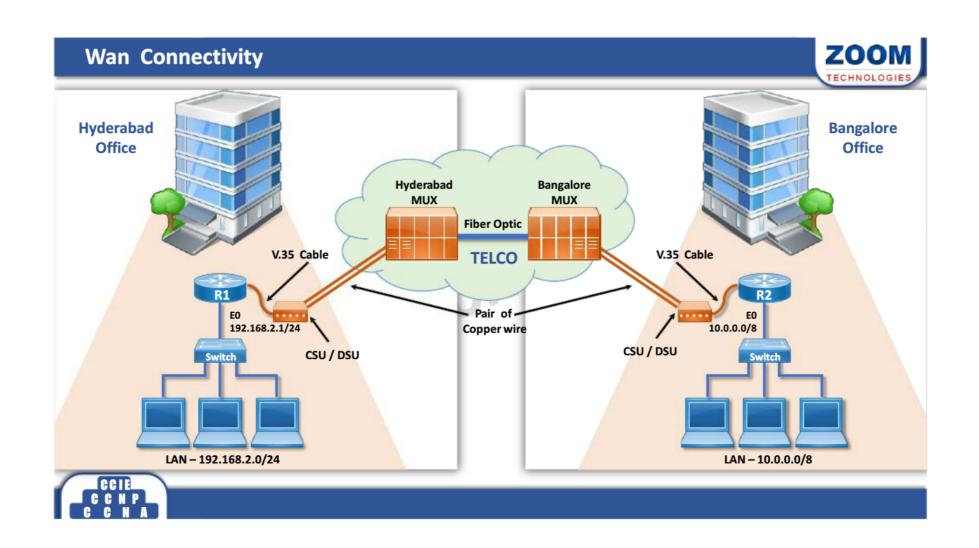


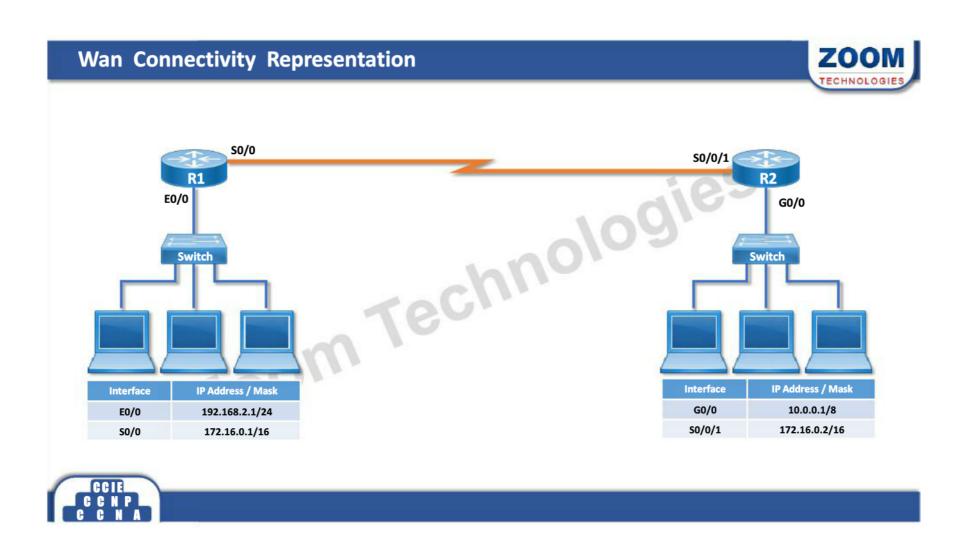
- Dedicated service
 - Leased Line
 - MLLN (Managed Leased Line Networks)
- · Circuit switching
- ogie⁵ - PSTN (Public Switched Telephone Networks)
 - ISDN (Integrated Services Digital Networks)
- Packet Switching
 - Frame-relay
 - MPLS (Multi Protocol Label Switching)
 - ATM (Asynchronous Transfer Mode)
- Broadband
 - DSL
 - Cable Internet
- VSAT



MOBILE - 3G/4G









Device Classification



DCE

- Data Communication Equipment
- Generate clocking (i.e. Speed)
- Master
- Example of DCE:- CSU/DSU

DTE

- Data Termination Equipment
- Accept clocking (i.e. Speed)
- Slave
- Example of DTE:- Router



Serial - back to back cable



- When the distance between two Routers is short, a special V.35 Back to Back Cable is used to replace the copper wire, CSU/DSU and MUX.
- For data communication using back to back Serial cable, one end has to be a DCE and the other has to be a DTE.





ROUTER 1



ROUTER 2





Encapsulation



- Encapsulation is the process of adding a new Header or Trailer to data.
- er transcondies The header and trailer contains information which is needed for proper transportation of the data.
- There are different types of WAN Encapsulation:
 - PPP
 - HDLC
 - Frame Relay



Wan Encapsulation



PPP

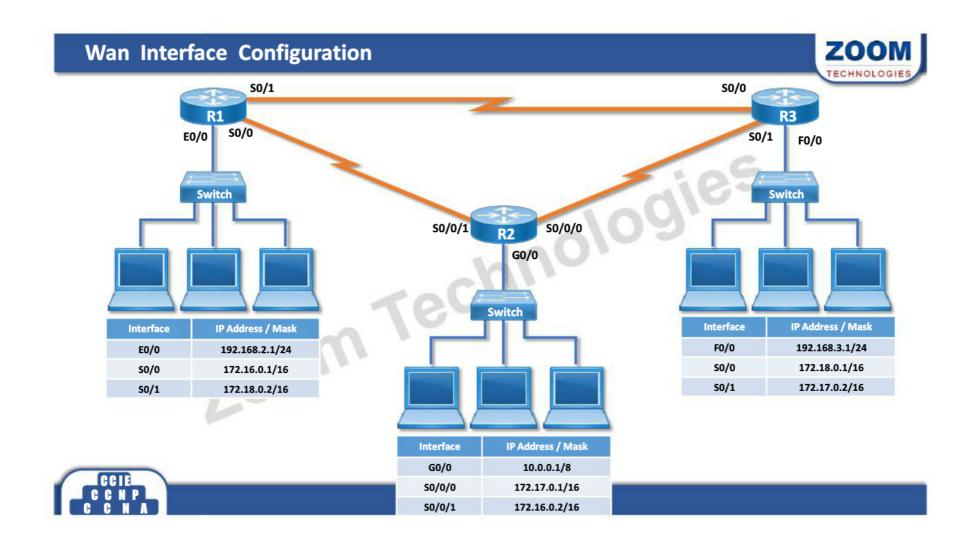
- **Point to Point Protocol**
- **Open Standard Protocol**
- **Supports Authentication**
- **Supports Compression**

HDLC

- High level Data link Control
- Vendor proprietary Protocol
- No Support for Authentication
- No Support for Compression







Serial Interface Configuration



To check DCE/DTE

Router# Show controllers Serial < no. >

Serial Interface Configuration

- Router(config)# interface Serial <no.>
- Router(config-if)# ip address < ip > < Subnet mask >
- Router(config-if)# no shutdown
- Router(config-if)# clock rate < bandwidth >
- Router(config-if)# encapsulation < HDLC/PPP >

Verification

Router# Show interface Serial <no. >







IP Routing



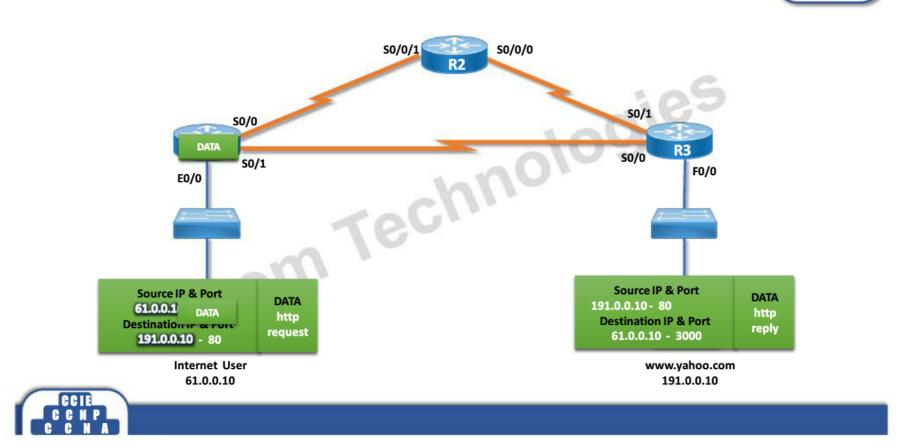
- · Routing is the process of moving IP packets from one network to another network.
- · Routing involves two basic activities:
 - Determining best paths.
- Zoom Technologies - Forwarding packets through these paths.

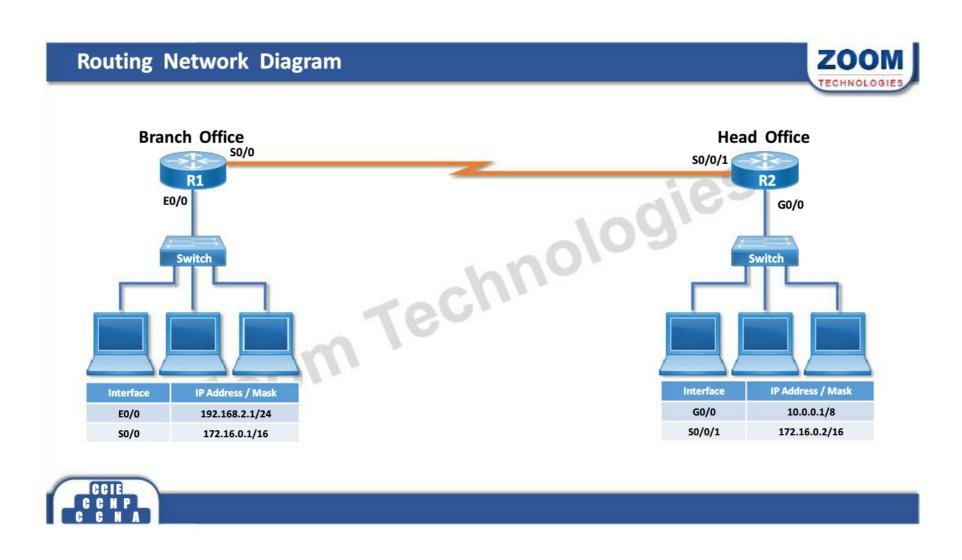




IP Routing







Conditions for Routing



- · The Head office router's Ethernet interface should be in the same network as the Head office LAN and similarly on Branch office side, the router's Ethernet interface should belong to the same network as the branch office LAN.
- · The serial interface between the head office and the branch office should be in same network.
- Head office LAN and Branch office LAN should be in different network.
- ulfei 700 All interfaces of a Router should be in different network.



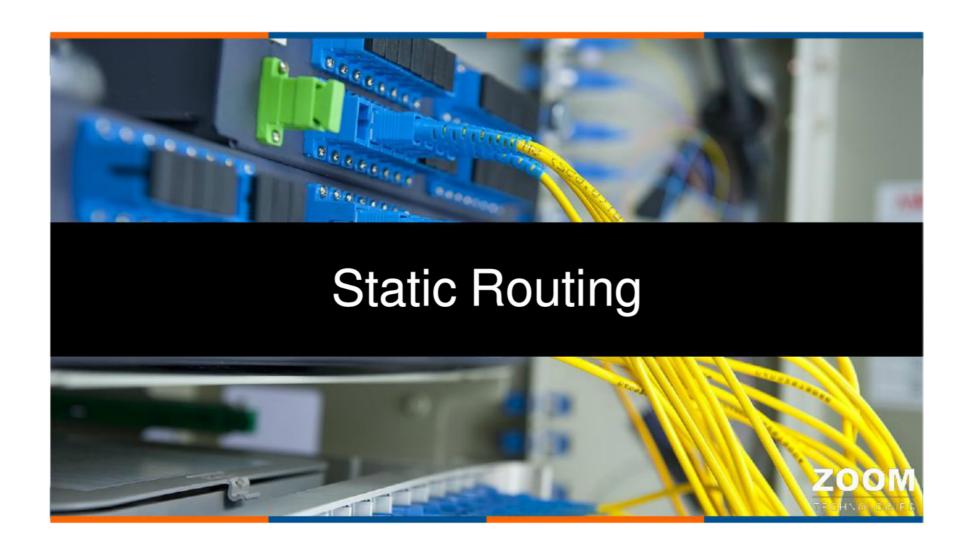
Types of Routing



- Static Routing
- Default Routing
- Zoom Technologies Dynamic Routing







Static Routing



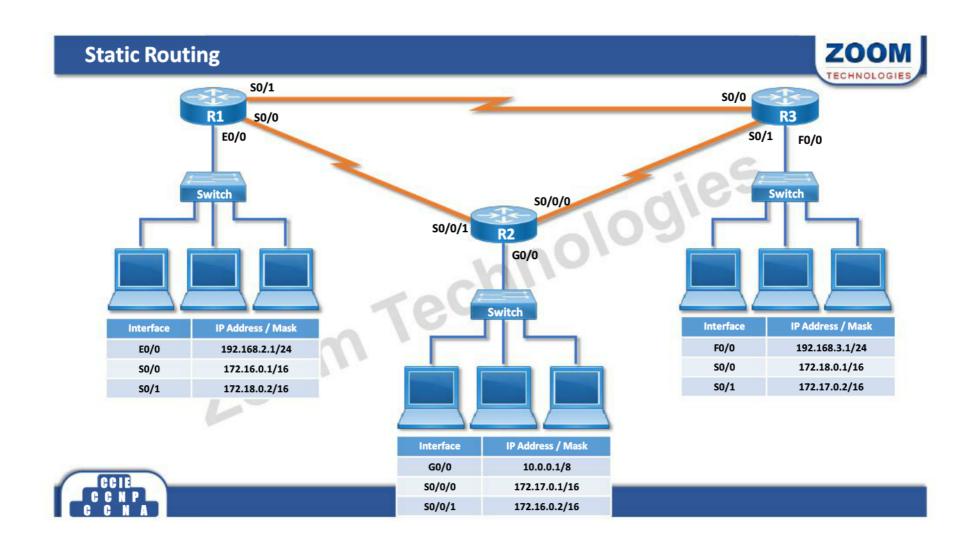
- Static routes are configured, maintained and updated by network administrator manually.
- · Administrator should know the destination IP network for configuration.
- Administrative distance for Static Route is 1.

200m

Administrative Distance (AD) is the "reliability" of the routing protocol. AD range is 0-255, lesser the administrative distance, higher the priority







Static Route Configuration



Static Route configuration

Router(config)# ip route < Destination network ID > < Destination
 Subnet mask > < Exit Interface type > < Exit interface no. >

Or

 Router(config)# ip route < Destination network ID > < Destination Subnet mask > < Next Hop IP address >

Verification

• Router# Show ip route

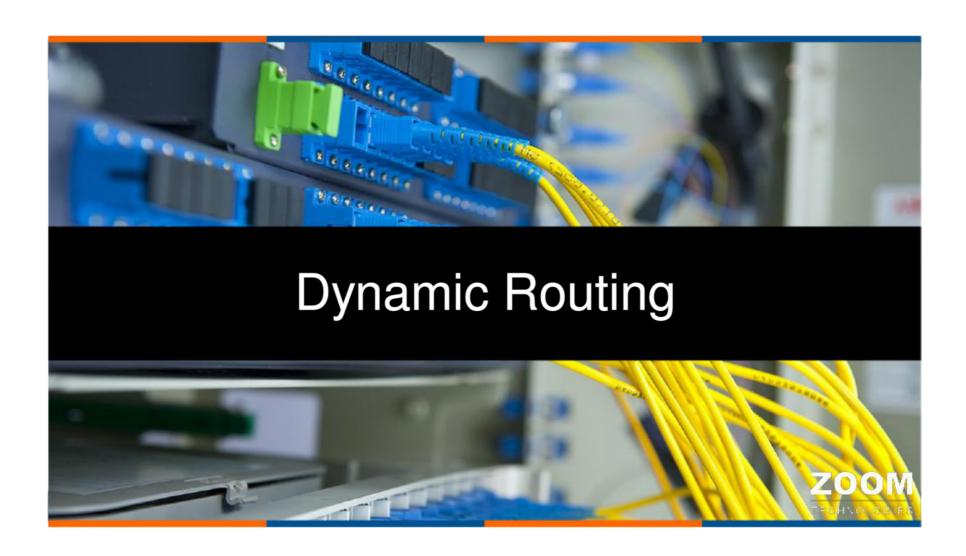


Advantages and Disadvantages of Static routing



Advantages	Disadvantages
Secured	No Automatic Updates
Reliable	Need of Destination network ID for the configuration
Faster	Administrative work is more
No wastage of bandwidth	Used in Small networks







Advantages of Dynamic routing



- Changes in the network topology are updated dynamically
- John Jechnologies 200 Only the directly connected network information is required for the configuration
- · Administrative work is reduced
- Used for medium and large Networks



Types of Dynamic Routing Protocols



- Distance vector
 - RIP (Routing Information Protocol)
 - IGRP (Interior gateway routing protocol)
- Advanced distance vector
- EIGRP(Enhanced Interior gateway routing protocol)

 Link-state
- Link-state
 - OSPF (open shortest path first)
 - IS-IS (intermediate system to intermediate system)







Routing Information Protocol



- Distance vector protocol
- It is open standard protocol
- · Uses Bellmen-ford Algorithm
- Classfull routing protocol
- Updates are periodically broadcasted using IP address 255.255.255.255
- Complete routing table sent as an update
- Each Update can contain maximum of 25 routes
- Administrative Distance is 120
- Metric is Hop count
- Maximum hop count supported is 15
- Load balancing on 4 equal paths by default (maximum 16 equal paths)
- Also known as "Routing by Rumor"





RIP Timers



Update Timer: 30 sec

Time between two consecutive updates

200m

• Invalid Timer: 180 sec

Time a router waits to hear an update from the neighbor The route is marked as unreachable if there is no update for this time period

• Flush Timer: 240 sec

Time after which the invalid route is removed from the routing table



Disadvantages of RIP



- More Bandwidth is utilized for sending the updates.
- , nop co Does not consider the bandwidth in metric calculations, uses only hop count
- Slow convergence
- Formation of routing loops





Routing loops



- Routing loops are formed due to the default behavior of RIP
- Zoom Technologies Complete routing tables are exchanged
- Slow convergence
- No verification of updates received



Routing loop avoidance



Built in Mechanisms to avoid switching loops

Split Horizon

A route learnt through an interface is never advertised back out of that same interface

Route poisoning

The route is marked as 16 hops

It is a mechanism to inform regarding unreachable route to neighbor

Poison reverse

Violating split horizon rule, sending the update through an interface from where it is being received, only in a case when network is unreachable (16hops)

· Hold down timer: 180 sec

The router does not accept any update for the invalid route for this time period

Flash update (Triggered update)

Change in the network topologies causes the router to send the update immediately without waiting for the update timer to get over



Comparison between RIPv1 and RIPv2



RIP v1

- Classfull routing protocol
- Does not advertise subnet mask information in routing update
- It works with broadcasting (255.255.255.255)
- It does not support Authentication

RIP v2

- Classless routing protocol
- Advertises the subnet mask information in routing update
- It works with multicasting (224.0.0.9)
- It supports Authentication



RIP configuration



RIP configuration

Router(config)# ip routing

Router(config)# router rip

Router(config-router)# network < Network ID >

Verification

Router# Show ip route

To check the logs

Router# debug ip rip
Router# terminal monitor

C C N P





Enhanced Interior Gateway Routing Protocol



gies

- Advance Distance vector routing protocol
- It is open standard protocol, was Cisco proprietary
- Uses DUAL (Diffusion Update Algorithm)
- Classless routing protocol
- Updates are sent through Multicast IP address (224.0.0.10)
- Incremental Updates and Triggered updates
- · Administrative distance is 90
- Metric : Composite Metric
 - Bandwidth, delay, load, reliability and MTU
 - Bandwidth and delay is used by default





EIGRP



- Maximum hop count supported is 255 (Default is 100)
- Hello packets are sent every 5 seconds
- Supports multiple Routed Protocols IP, IPX and Apple Talk protocols
- Support equal and unequal cost load balancing (default 4 paths and maximum 16 zoom Technol equal or unequal path)
- Fast Convergence to topology changes



EIGRP Tables



- Neighbor Table
 - Contains information about directly connected neighbors.
- Topology Table
 - Contains entries for all destinations, along with the feasible distance and the advertised distance.
 - Contains the successors.
 - Contains feasible successor if any.
- Routing Table
 - Entries with the best path for each destination from the Topology table are moved into the Routing Table





EIGRP Terminology

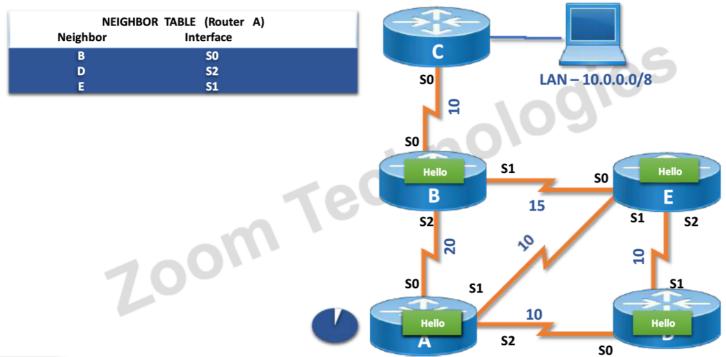


- Feasible Distance FD :
 - Feasible distance (FD) is the metric of the best route to a destination, including the local link distance.
 - Feasible distance = advertised distance + local link distance (of the best path)
- Advertised Distance AD:
 - The distance of a route as advertised by the neighbor. It does not include the local link distance.
- Successor:
 - The neighbor with best distance to the destination.
- Feasible Successor:
 - The neighbor with second best distance to the destination, which meets this criteria: advertised distance should be less than the feasible distance (AD <FD)



EIGRP - Neighbor Table



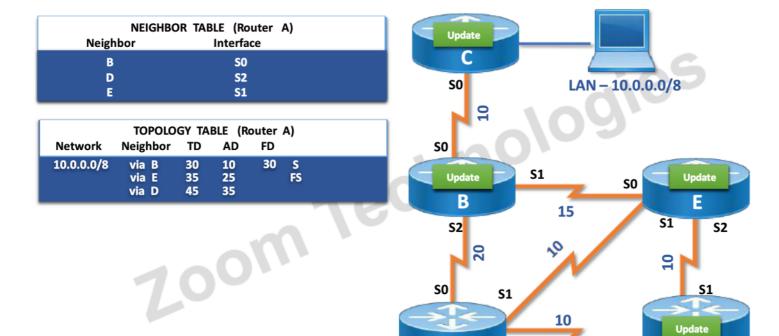






EIGRP - Topology Table







EIGRP - Routing Table



NEIGHBOR TABLE (Router A) Neighbor Interface	
B S0 D S2 E S1	S0 LAN - 10.0.0.0/8
TOPOLOGY TABLE (Router A) Network Neighbor TD AD FD	SO SO
10.0.0.0/8 via B 30 10 30 S via E 35 25 FS via D 45 35	S1 SO E
ROUTING TABLE (Router A) D 10.0.0.0/8 [90/30] via B, 01:36, Serial0	S2 S1 S2
	S0 S1 S1
	A S2 S0 D



Autonomous System



- · An autonomous system is a collection of networks or routers under a common administrative policy Zoom Technologies
- Autonomous systems are identified using numbers
- Autonomous system number ranges from 0 65535

Public

- Private



Routing Protocol Classification



IGP

- Interior Gateway Protocol
- Routing protocols used within an **Autonomous system**
- Ex: RIP, IGRP, EIGRP, OSPF, IS-IS

EGP

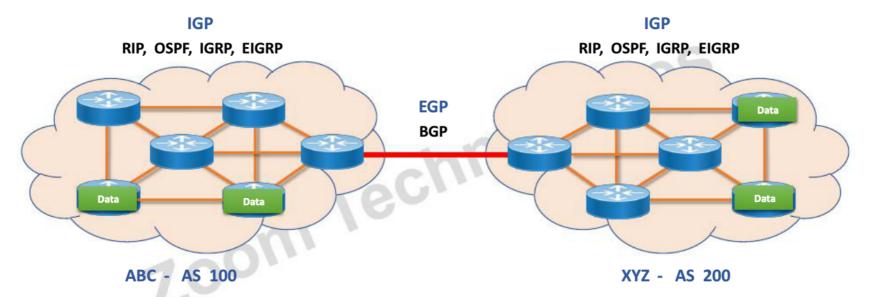
- **Exterior Gateway Protocol**
- Routing protocol used between different Autonomous systems
- Ex: Border Gateway Protocol is extensively used as EGP





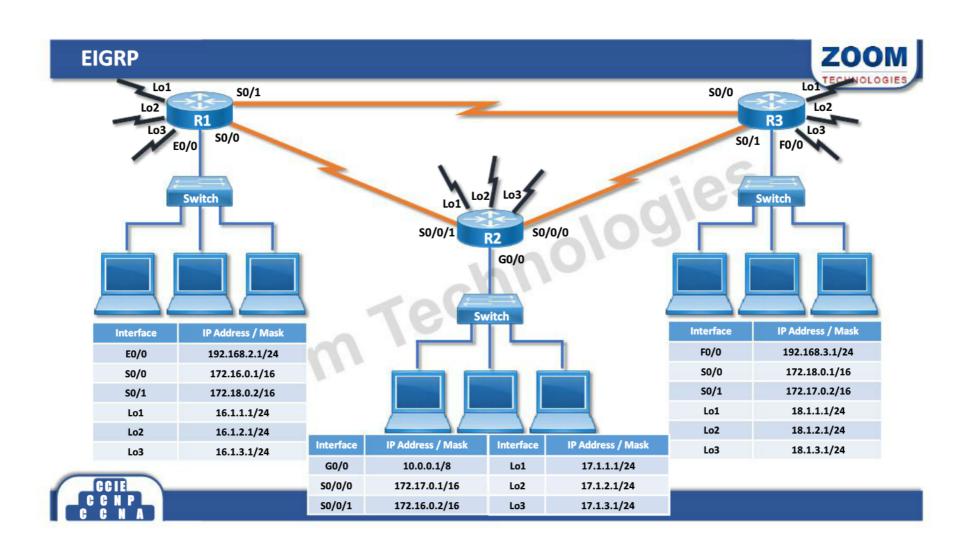
IGP and **EGP**





- IGPs operate within an autonomous system
- EGPs connect different autonomous systems





Eigrp configuration and Verification Syntax



EIGRP configuration

- Router(config)# ip routing
- Router(config)# router eigrp <As no. >
- Router(config-router)# network < Network ID >

Verification

To check Routing Table

Router # show ip route

To check Neighbor Table

Router # show ip eigrp neighbor

To check Topology Table

Router # show ip eigrp topology



Summarization



- Route summarization takes a set of contiguous networks or subnets and groups them together using a shorter subnet mask.
- The advantages of summarization are that it reduces the number of entries in the route table.





OTHER EIGRP FUNCTIONS



- EIGRP supports Auto-summarization and Manual summarization.
- Zoom Technologies EIGRP support unequal-cost load-balancing
- EIGRP supports passive-interface



EIGRP summarization



- EIGRP supports summarization at any location in the internetwork.
- By default EIGRP has auto-summarization enabled.

Zoom

· Summarize the routes that are advertised through classfull network boundaries.

To disable auto-summarization Router(config)# router eigrp <As. no.> Router(config-router)# no auto-summary





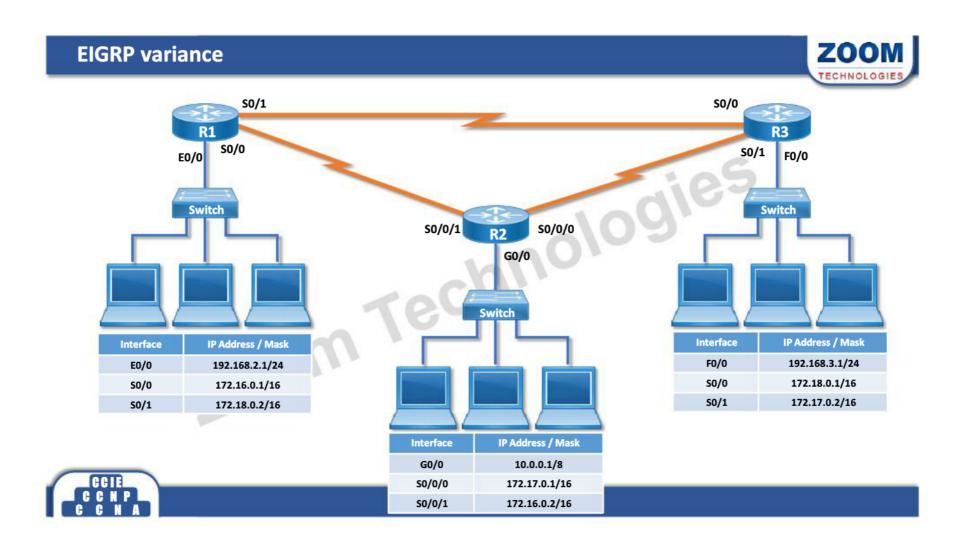
EIGRP Unequal Cost Load balancing



- Every routing protocol supports equal cost path load balancing.
- EIGRP also support unequal cost path load balancing.
- To configure unequal cost load balancing, next available paths should be feasible successors.
- Unequal cost load balancing can be configured by using "Variance"
- Default Variance value is 1 (Equal cost load balancing)

To configure variance
Router(config)# router eigrp <As. no.>
Router(config-router)# variance <1-128>







EIGRP Passive interface



- The interface can be configured as passive, for stopping the hellos and Updates.
- The passive interface cannot send any hellos over the interface, but it can receive hellos.

To configure passive interface

Router(config)# router eigrp <As. no.>

Router(config-router)# passive-interface <interface type> <no.>







Open Shortest Path First



- Link State Protocol
- Open standard
- Classless routing protocol
- Uses Dijkstra (Shortest Path First (SPF)) Algorithm
- Updates are sent through Multicast IP address 224.0.0.5 and 224.0.0.6
- Supports Triggered Updates and incremental updates
- Administrative distance is 110
- Metric = Cost = 10⁸/Bandwidth in bps (CISCO)



OSPF (contd..)



- Hello packets are sent every 10 seconds, Dead interval 40 sec
- OSPF sends updates (LSAs) when there is a change to one of its links gies
- LSAs are additionally refreshed every 30 minutes.
- Unlimited Hop Count
- Designed to scale and support large / Enterprise networks
- Hierarchical network design using Areas
- One area has to be designated as Area 0
- Area 0 is called the Backbone Area oom

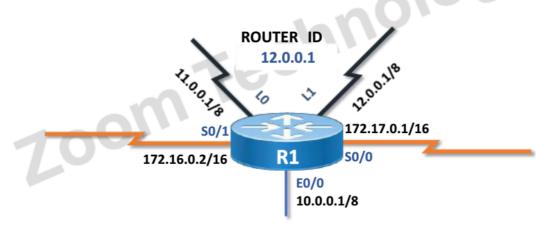




Router ID



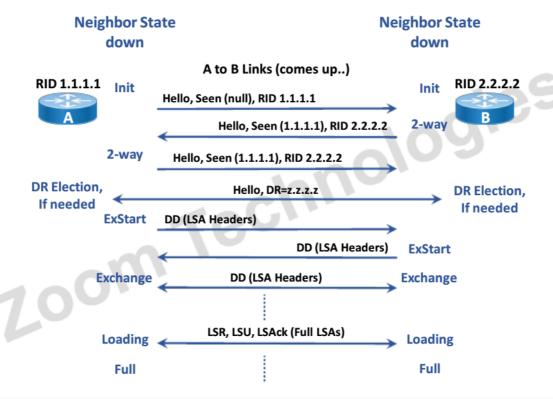
- Router ID is used to identify the Router.
- The highest IP assigned to an active physical interface is the Router ID.
- If logical interface is configured then the highest IP assigned to a logical interface (loopback) is the Router ID.





OSPF Neighbor States









OSPF Terminology



- Neighbor
 - Routers that share a common link become neighbors.
 - Neighbors are discovered by Hello Packets.
 - echnologie⁵ - To become neighbors the following should match
 - Area ID
 - Network ID and Subnet Mask
 - · Hello and Dead Intervals
 - Authentication
- Adjacencies
 - Adjacencies are formed once neighbor relation is established.
 - In Adjacencies the database details are exchanged.



OSPF Tables



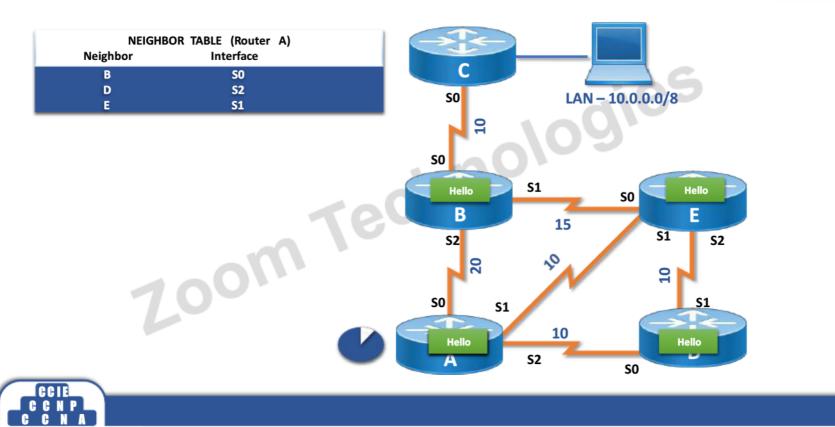
- It maintains three tables:
- Neighbor Table
 - Neighbor table contains information about the directly connected OSPF neighbors forming adjacency.
- Database Table
 - Database table contains information about the entire view of the topology with respect to each router.
- Routing Table
 - Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.





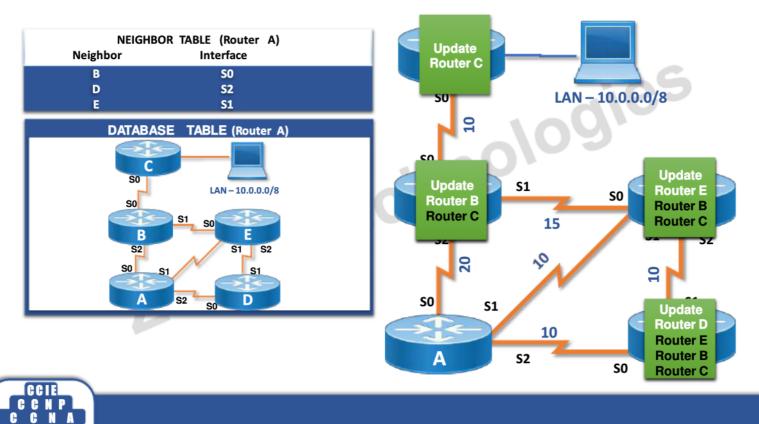
OSPF - Neighbor Table





OSPF - Database Table

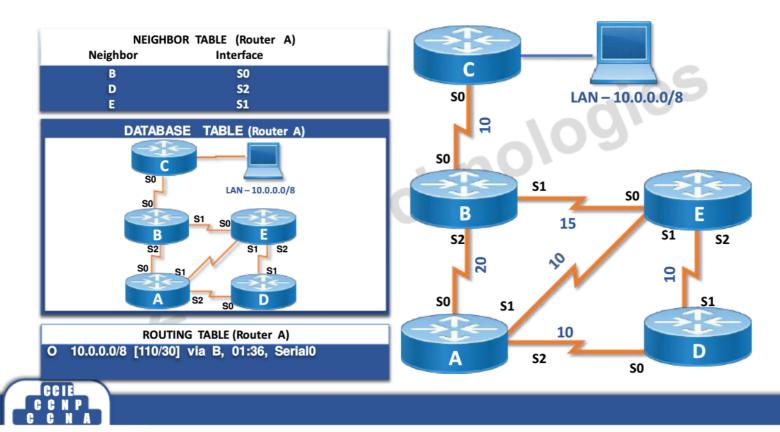






OSPF - Database Table





Wild Card Mask



· A wild card mask can be calculated using the formula:

Global Subnet Mask

Subnet Mask

Wild Card Mask

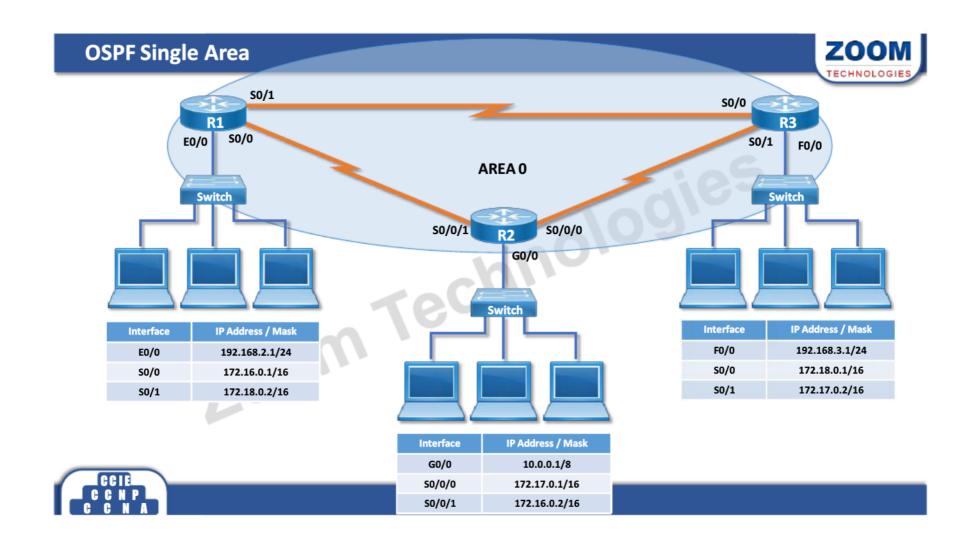
0.

E.g.

- chnologies 255.255.255 255.255.255 255.255.255. 0 255.255.255.240
 - 0. 0.255 0. 0. 0. 15







OSPF configuration and Verification syntax



OSPF configuration

- Router(config)# ip routing
- Router(config)# router ospf < Process ID >
- Router(config-router)# network < Network ID > <Wildcard mask > area <area ID >

Verification

To check Routing Table

• Router # show ip route

To check Neighbor Table

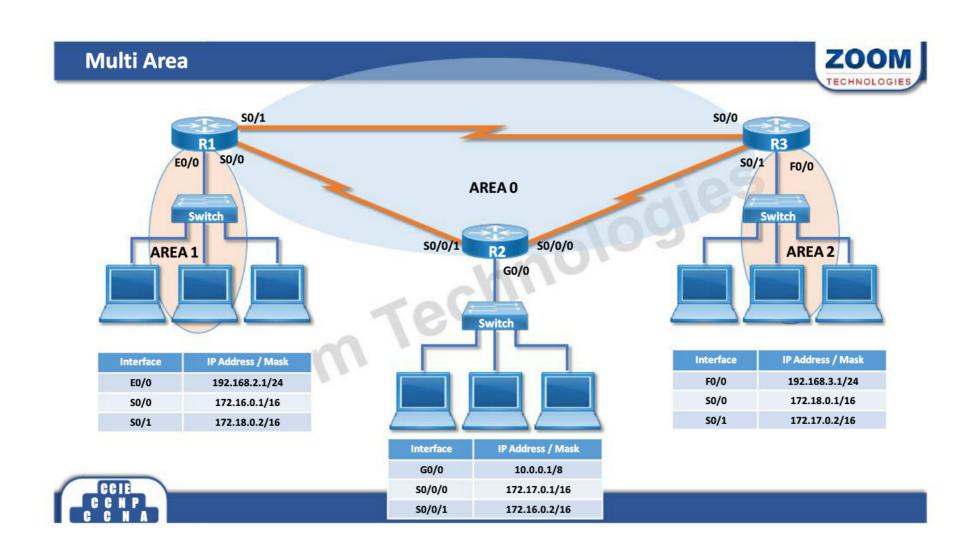
• Router # show ip ospf neighbor

To check Database Table

• Router # show ip ospf database

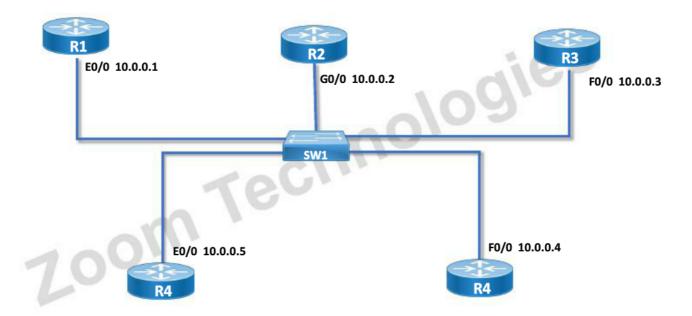






OSPF in LAN









DR and BDR



- Designated Router (DR)
 - Designated Router is elected when ever OSPF routers are connected to the same multi-access networks.
 - This is done to reduce the number of adjacencies formed.
 - If there is a change in topology the initial router will only update the DR and BDR and no other router. The DR in turn will update the remaining routers.
- Backup Designated Router (BDR)
 - This is a backup to the DR and will only receive updates but will not update the other routers.
 - If the DR goes down then the BDR will act as the DR.



DR and BDR Elections



- DR and BDR Election is done by the Hello Packets
- The router with the highest OSPF priority will become the DR and the router with the second highest priority will become BDR
- On all routers the default priority is 1
- In that case, the router with the highest Router ID will become the DR and the Router with the second highest ID will become the BDR
- Multicast address used for updating
 - Other routers to DR → 224.0.0.6
 - DR to other routers → 224.0.0.5





DR and BDR



To check DR/BDR status

To check DR/BDR Status

• Router # show ip ospf neighbor

To check the self status

• Router # show ip ospf interface ethernet < no. >

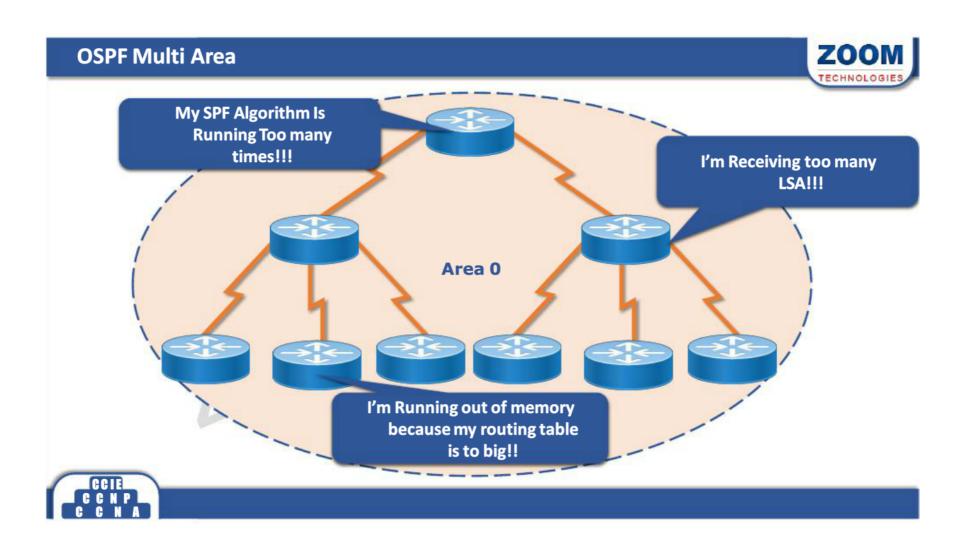
To change the priority

- Router(config) # interface ethernet < no. >
- Router(config-if) # ip ospf priority < priority >

For Election process

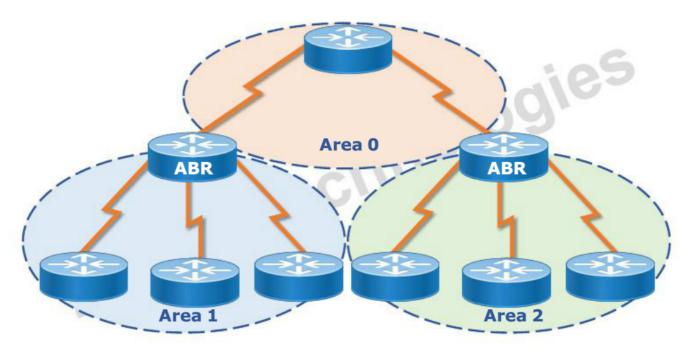
Router # clear ip ospf process





Issue of Maintaining of large OSPF network







ABR and ASBR



- ABR (Area Border Router)
 An OSPF Router with interfaces connected to the backbone area and to other area
- ASBR (Autonomous System Border Router)
 A router that exchanges routing information with routers belonging other AS (Autonomous System)







LSA Types	Name
1	Router LSAs
2	Network LSAs
3	Summary LSAs



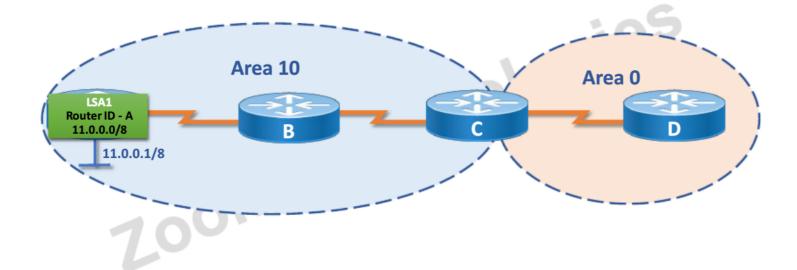


- One Router LSA (type 1) for every router in an area
 - Includes list of directly attached links
 - Each link identified by IP prefix and link type
- ..e ABR Identified by the router ID of the originating router
- Floods within its area only; does not cross the ABR











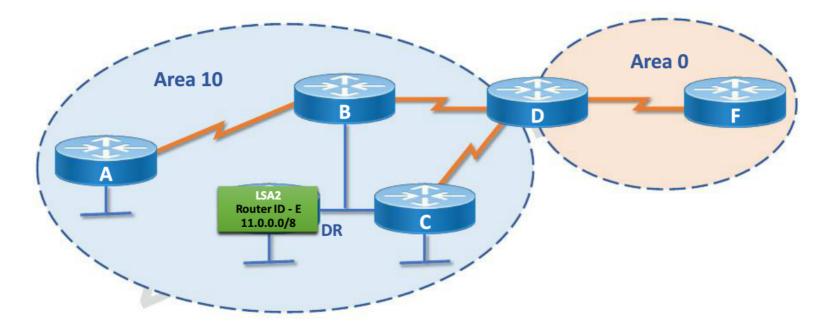


- · One Network (type 2) LSA for each transit broadcast or NBMA network in an area .crans Includes Network ID, subnet mask and list of attached routers on that transit link
- Advertised by the DR of the transit network
- · Floods within its area only; does not cross ABR











LSA Type - 3

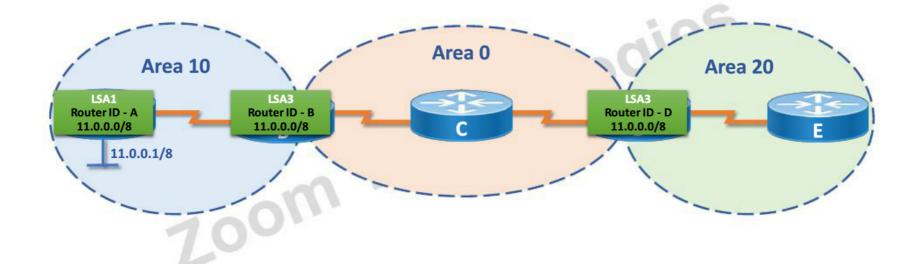


- Type 3 LSAs are used to flood network information to areas outside the originating area (inter-area)
 contains network ID and subnet mask
- Advertised by the ABR of originating area
- · Regenerated by subsequent ABRs to flood throughout the autonomous system.
- By default, routes are not summarized and there is one type 3 LSA for every subnet











Disadvantages of OSPF



- Consumes More Memory and CPU processing time
- Complex configuration





Access Control List



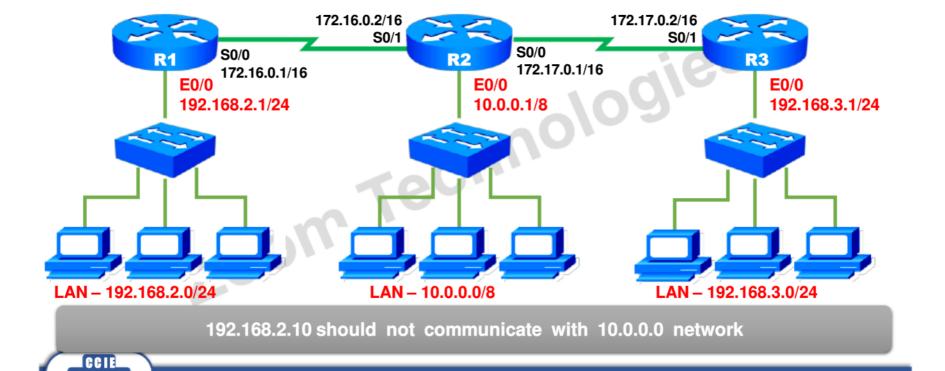
- · Access Control List provides network security.
- It provides layer 3 and layer 4 security.
- 7.00m Technologies • Controls the flow of traffic from one network to another.
- Filters IP Packets (Packet Filtering Firewall)





ACL - Network Diagram





Terminology



- Deny: Blocking a network/subnet/host/service.
- Permit : Allowing a network/subnet/host/service.
- Source Address: The address from where the request starts.
- Destination address: The address where the request ends.
- · Inbound: Traffic coming into the interface.
- Outbound: Traffic going out of the interface.



Terminology



- Protocols: IP (Internet Protocol)
 - TCP (Transmission control protocol)
 - UDP (User datagram protocol)
 - ICMP (Internet control messaging protocol)
- Operators:
 - eq (equal to)
 - neq (not equal to)
 - It (less than)
 - gt (greater than)
- echnologies Services: HTTP (80), FTP (20,21), TELNET (23), DNS (53), DHCP (67,68)



Wildcard Mask



logies

- It's the inverse of the subnet mask, hence is also called as inverse mask.
- A bit value of 0 indicates MUST MATCH (Check Bits).
- A bit value of 1 indicates IGNORE (Ignore Bits).
- Wildcard Mask for a host is 0.0.0.0
- Wildcard Mask for Class A network is 0.255.255.255
- Wildcard Mask for Class B network is 0.0.255.255
- Wildcard Mask for Class C network is 0.0.0.255

Zoom





Wild Card Mask



· A wild card mask can be calculated using the formula:

Global Subnet Mask

Subnet Mask

Wild Card Mask

E.g.

255.255.255.255

- 255.255.255. 0

0. 0. 0.255

255.255.255

- 255.255.255.240

0. 0. 0. 15



Working of Access Control List



- Works in a sequential order from top to bottom.
- If a match is found it does not check further.

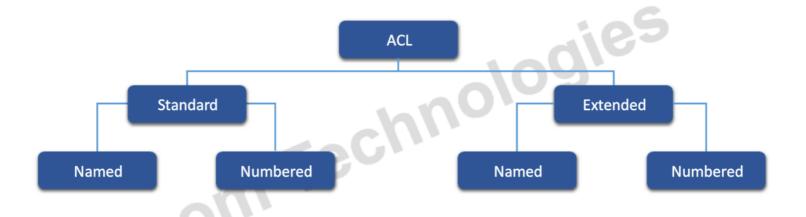
oom

- · There should be at least one permit statement.
- An implicit deny blocks all traffic by default when there is no match (an invisible statement).
- New entries are automatically added to the bottom.
- Can have one access-list per interface per direction.
- Removing of specific statement in a numbered access-lists is not possible.



Types of Access-List







Standard Access List



- The access-list number range is 1 99.
- Can filter a network, subnet or host.

- traffic based only on the source address.

 Implemented closest to the destination. (Guideline) ..on. (Guid





Standard Access Control List Configuration



Creation of Standard Access List

Router(config)# access-list <acl no> <permit/deny> <source address> <source wildcard mask>

Implementation of Standard Access List

Router(config)# interface <interface type> <interface no> Router(config-if)# ip access-group <number> <out/in>

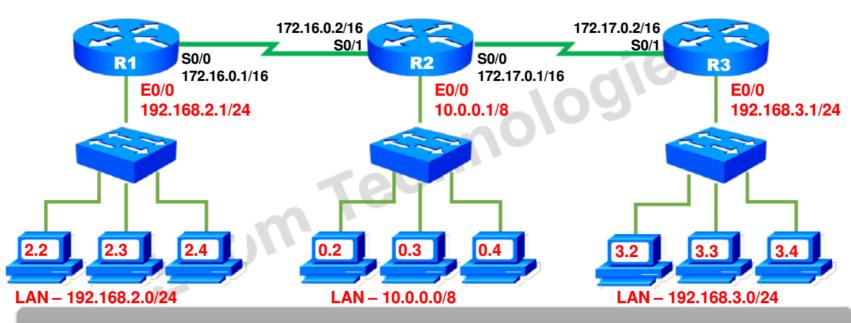
Verification

Router# Show access-list



Standard ACL - Network Diagram



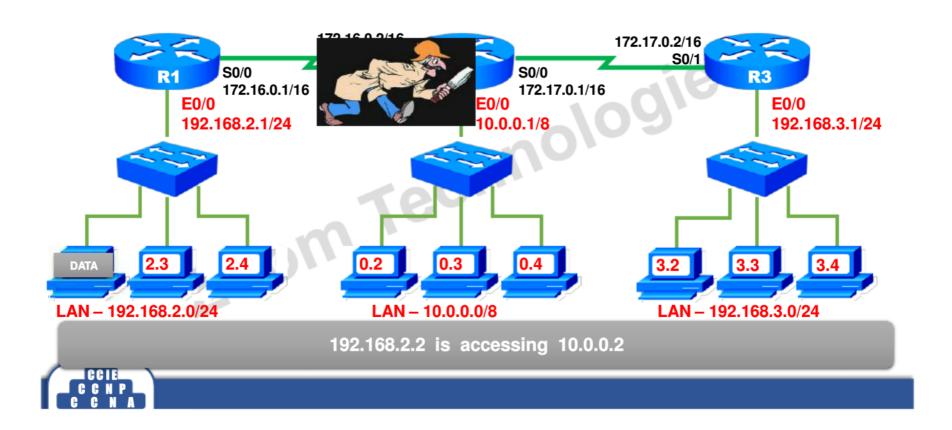


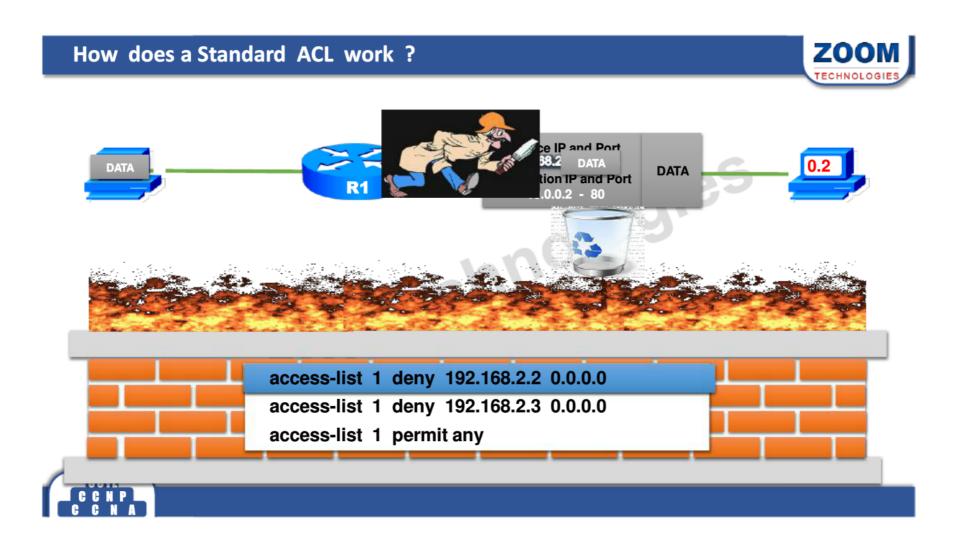
192.168.2.2 and 192.168.2.3 should not communicate with 10.0.0.0 network



How does a Standard ACL work?

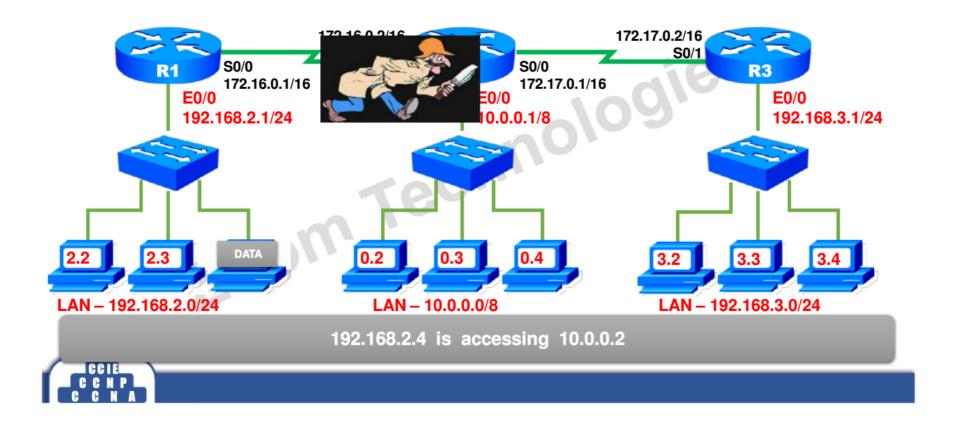






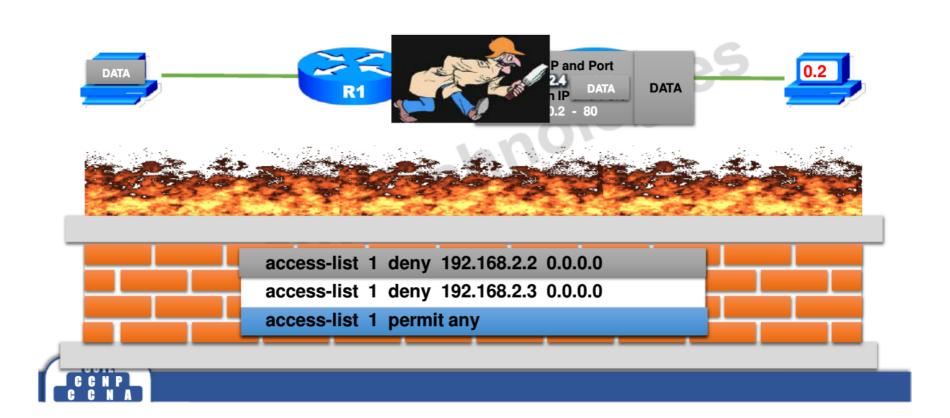
How does a Standard ACL work?





Example of a standard access list





Extended Access List



- The access-list number range is 100 199.
- Can filter a network, subnet, host and service.
- One way communication is stopped.
- Selected services can be blocked or allowed.
- · Filters traffic based on the source address, destination address and service.
- Implemented closest to the source. (Guideline)



Extended Access Control List configuration



Creation of Extended Access List

Router(config)# access-list <acl no> <permit/deny> <protocol> <source address> <source wildcard mask> <destination address> < destination wildcard mask> <operator> <service>

Implementation of Extended Access List

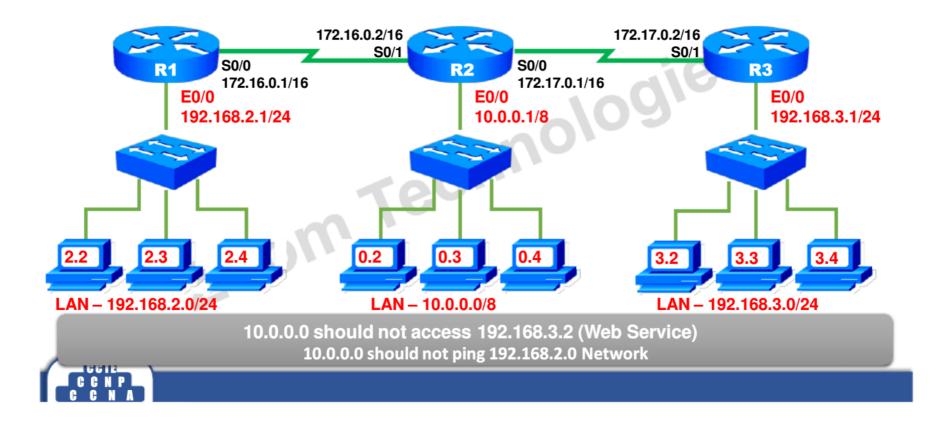
Router(config)# interface <interface type> <interface no> Router(config-if)# ip access-group <number> <out/in>

Verification

CC IE C C N P C C N A **Router# Show access-list**

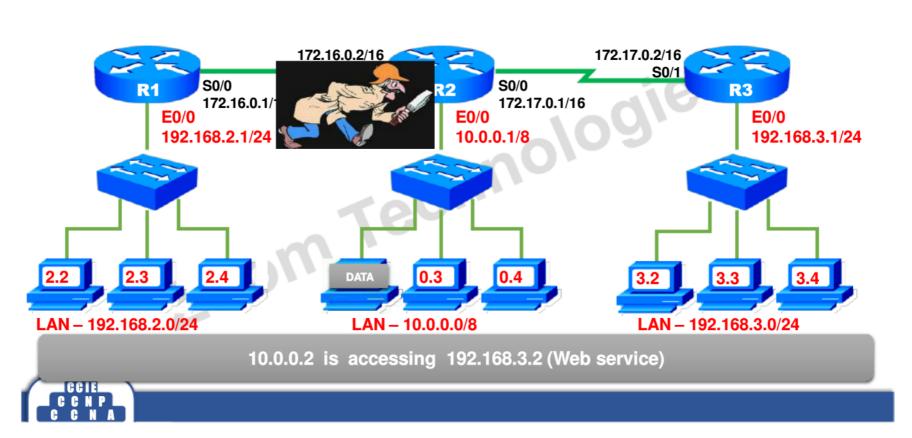
Extended ACL - Network Diagram





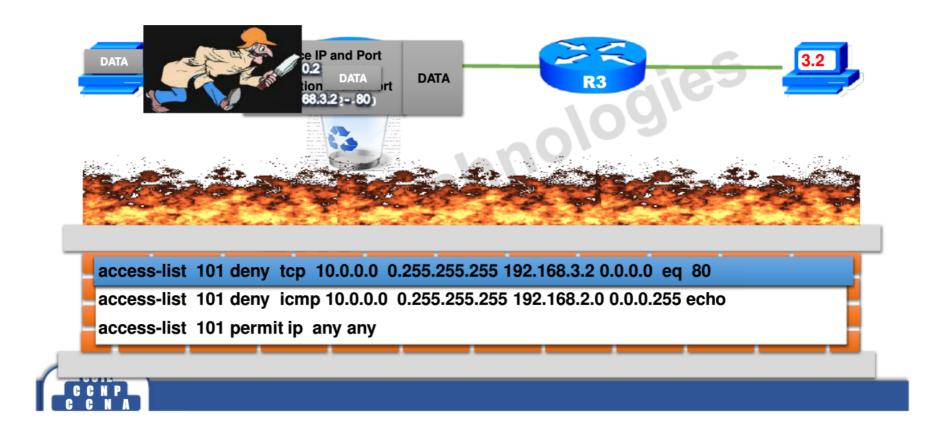
How does an Extended ACL work?





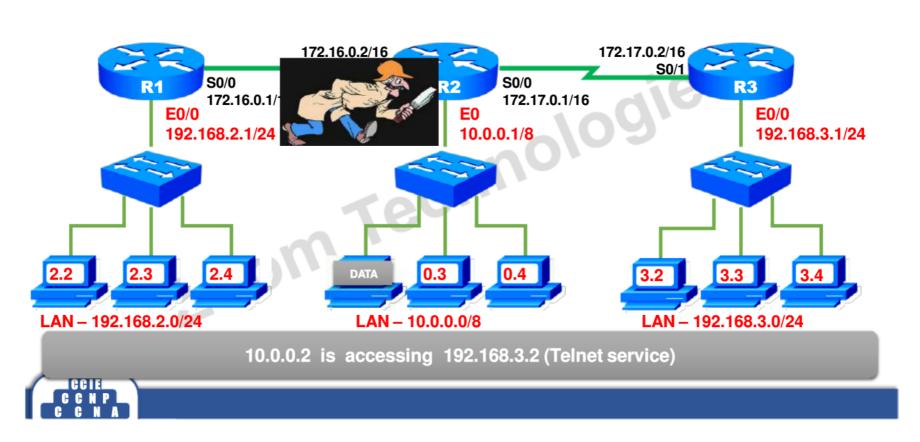
How does an Extended ACL work?





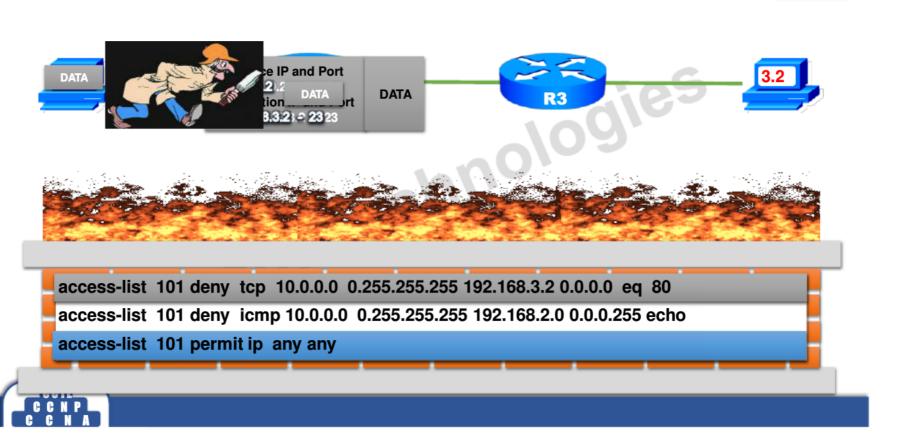
How does an Extended ACL work?





How does an Extended ACL work?









Broadcast and Collision Domain

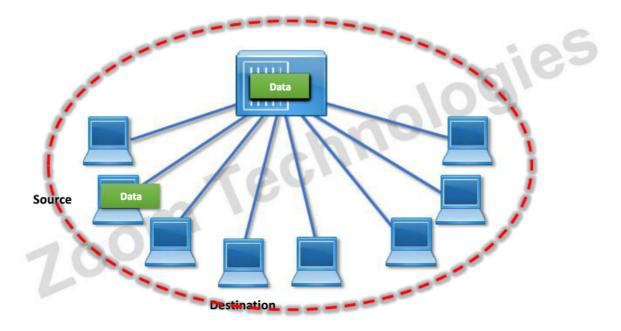


- Broadcast Domain: A broadcast domain is a set of network devices for which a broadcast frame sent by one device is received by all other devices in that LAN segment.
- Collision Domain: A collision domain is a set of network devices for which a frame sent by one device could result in a collision with a frame sent by any other device in the same LAN segment.



Functions of HUB



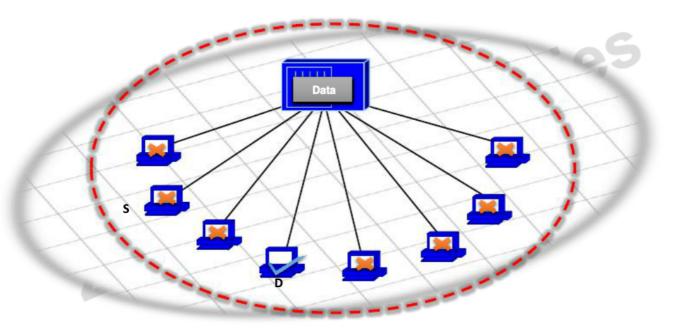






Functions of HUB

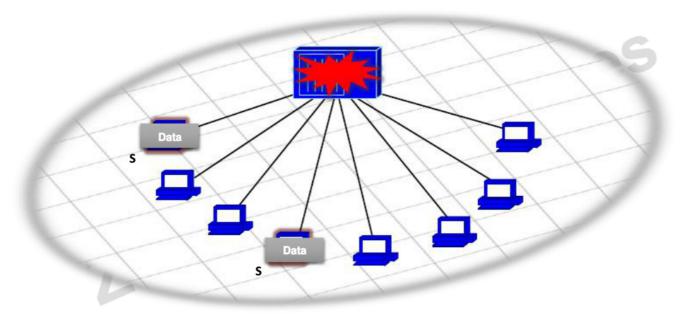






Functions of HUB



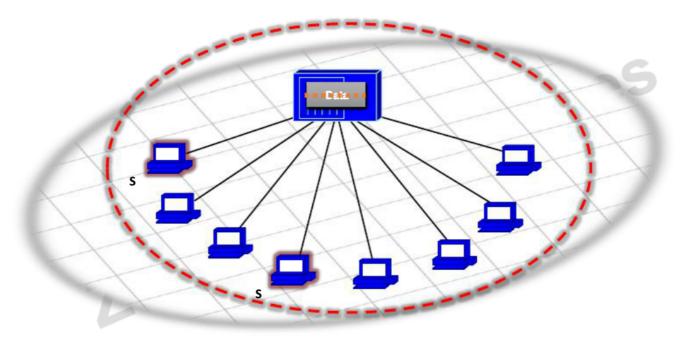






Functions of HUB

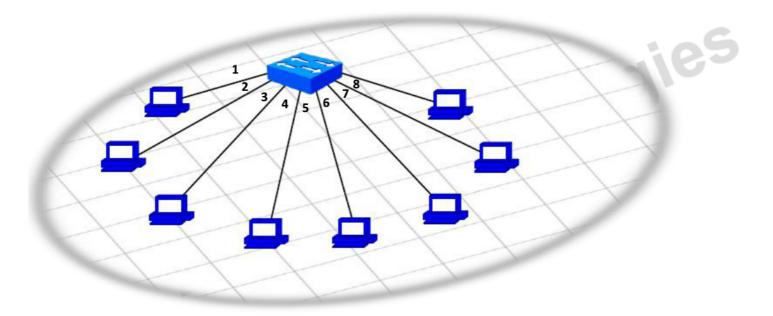






Functions of Switch



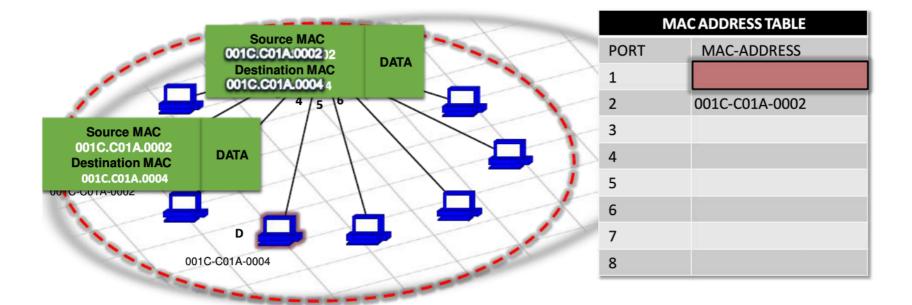






Functions of Switch

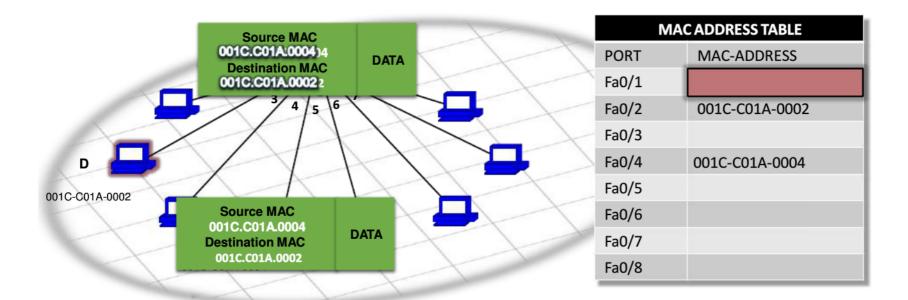






Functions of Switch









Types of Switches



- Manageable switches
 - On a Manageable switch an IP address can be assigned and configurations can be made. It has a console port.
- Unmanageable switches
 - not be - On an Unmanageable switch configurations cannot be made, an IP address cannot be assigned as there is no console port.



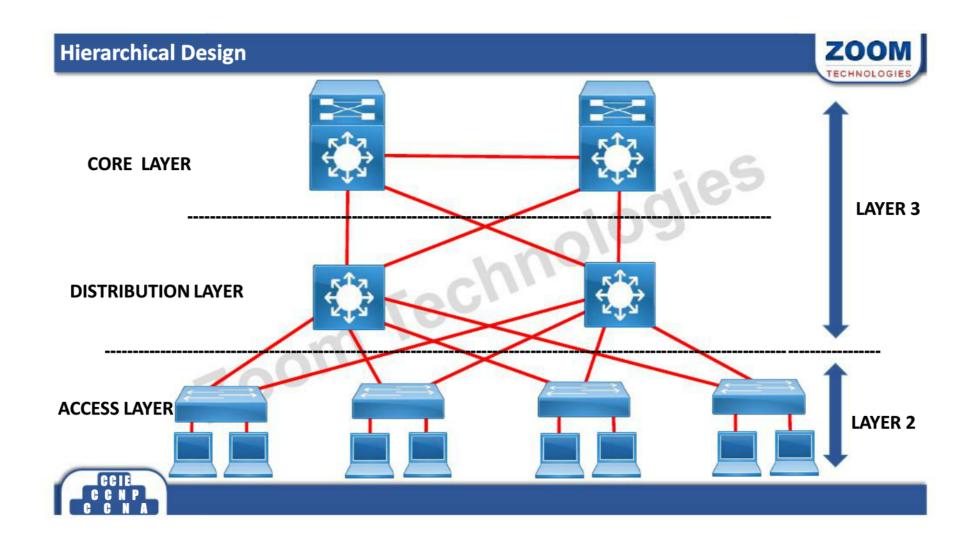
Campus Network



- Campus is a LAN network supporting larger buildings or multiple buildings close to a specific area
- Lampus d Cisco uses three terms to describe the role of each switch in a campus design
 - Access
 - Distribution
 - Core







Cisco's Hierarchical Design for switches



- Cisco Switches can be categorized into 3 Layers
 - Access Layer Switches Switches Series: 1900, 2950, 2960
 - rechnologies
 - Distribution Layer Switches **Switches Series:**
 - Fixed: 3550, 3560, 3750 • Modular: 4500, 5500
 - Core Layer Switches **Switches Series: 6500**







Virtual LAN



- Divides a Single Broadcast domain into Multiple Broadcast domains
- provides L2 Security
- ...wn a • By default all ports of the switch are in VLAN1 . VLAN1 is known as Administrative **VLAN or Management VLAN**
- VLAN can be created from 2 1001





Static VLAN



- Static VLANs are port based hence they are also called as Port-based VLANs.
- Zoom Technologies Ports have to be manually assigned to a VLAN.
- A Port can be a member of a single VLAN.



Dynamic VLAN



- Dynamic VLANs are based on the MAC address of a device
- Switch automatically assigns the port to a VLAN
- Each port can be a member of multiple VLAN's
- MPS(VL For Dynamic VLAN configuration, a software called VMPS(VLAN Management Policy Server) is needed







Creating VLAN

Switch(config)# Vlan < vlan number > Switch(config-vlan)# name < name >

Implementation of Vlan

Switch(config)# interface <interface type> <interface no> Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan < Vlan ID > Switch(config-if)#exit

Verification

Switch# Show vlan brief



Trunk



· Trunk Port allows multiple Vlan traffic to pass through a single physical connection by adding a header to Ethernet frame.

Trunking Protocols of two different types

nking Protocols of two different type	es logies
ISL(Inter Switch Link)	802.1q
Cisco proprietary	Open standard
30 bytes	4 bytes
7.00m	





Trunk configuration



Trunk configuration

Switch(config)# interface <interface type> <interface no>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan < all/vlan ID >
Switch(config-if)#exit

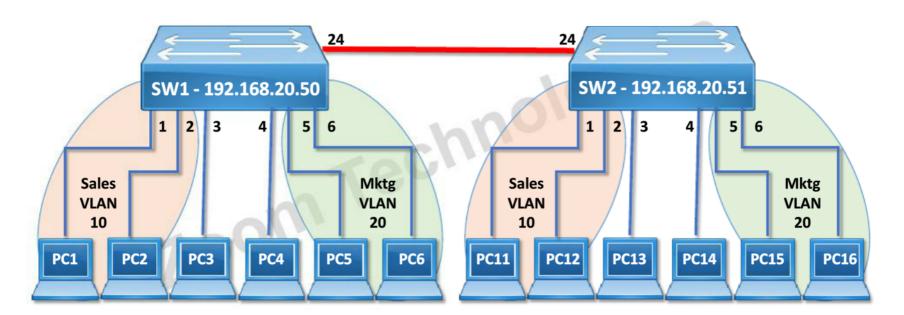
Verification

Switch# Show interface trunk



VLAN and Trunk









Dynamic Trunking Protocol (DTP)



- DTP is a Cisco proprietary protocol.
- zoom Technologies • DTP is responsible for dynamically negotiates trunks between Switches.
- DTP is enabled in all Cisco switches by default.
- DTP modes
 - Access mode
 - Trunk mode
 - Dynamic desirable
 - Dynamic auto



DTP Modes



Command Option	Description	
Access	Always act as an access(Non-Trunk) port	
Trunk	Always act as a Trunk port	
Dynamic Desirable	Initiates negotiation messages and responds to negotiation messages to start using Trunking	
Dynamic Auto	Passively waits to receive trunk negotiation messages	







Administrative mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
Access	Access	Access	Do not Use	Access
Dynamic Auto	Access	Access	Trunk	Trunk
Trunk	Do not Use	Trunk	Trunk	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk





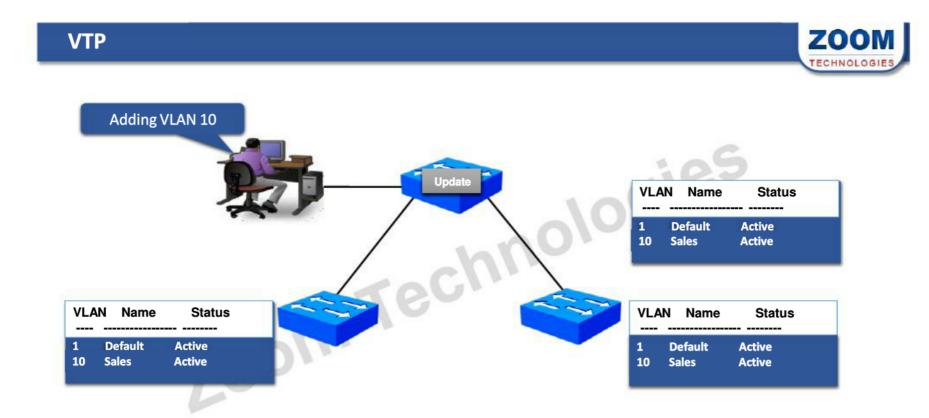


Virtual LAN Trunking Protocol (VTP)



- VTP is a CISCO proprietary protocol
- It is used to share the VLAN configurations with multiple switches
- The new VLAN needs to be added only on one switch and the configuration will automatically be sent to all other switches
- VTP only works when trunking is configured on FastEthernet or higher ports
- Note: Switches Should be configured with same Domain Name. Domain Names are Case sensitive









VTP Modes



- Server
 - Default mode
 - Create, Modify and Delete VLANs
- Client
- Transparent
- Cannot create, Modify or delete VLANs
 forwards advertisements
 Synchronizes

 Transparent
 Creat - Create , Modify and Delete local VLANs only
 - Forwards advertisements
 - Does not synchronize



VTP configuration



Configuring VTP

Switch(config)# VTP Mode < server/client/transparent >

Switch(config)# VTP Domain < Name >

Switch(config)# VTP Password < password >

Verification

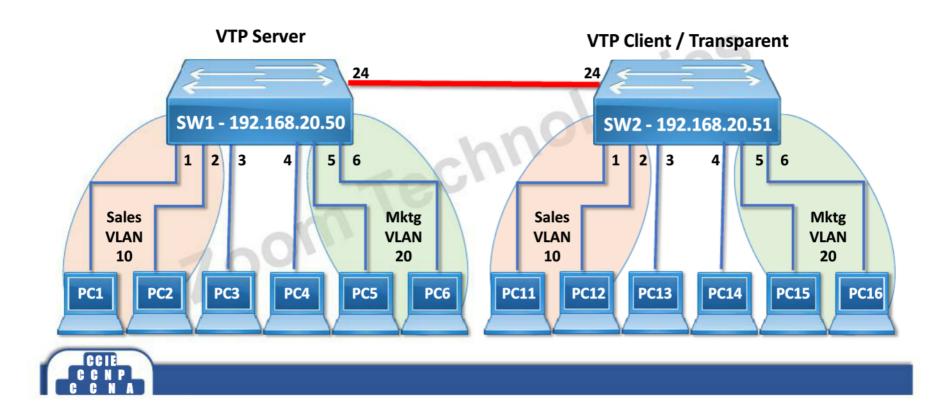
Switch# Show vtp status Switch# Show vtp password





VLAN Trunking Protocol









Inter-VLAN Routing

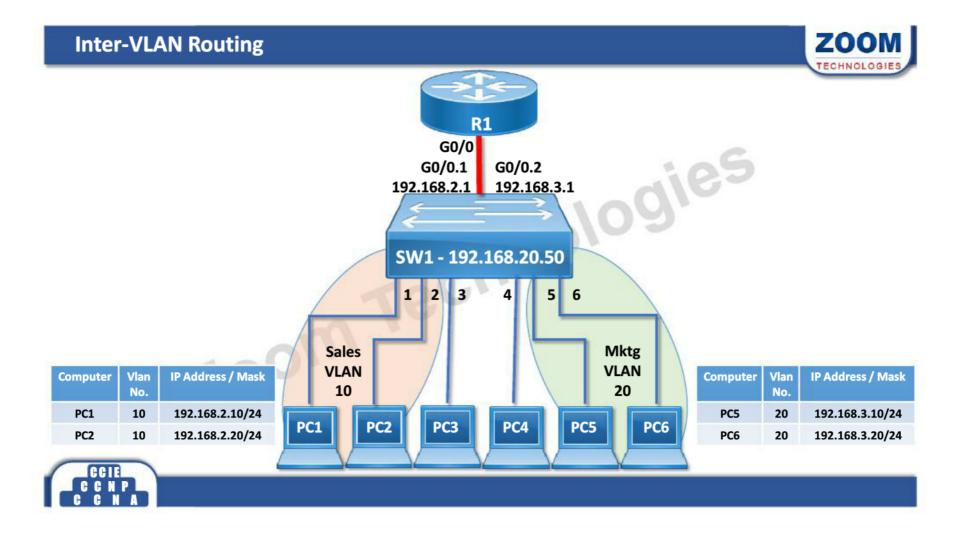


- Inter-VLAN routing is a process of forwarding network traffic from one VLAN to another
- · Layer-3 device is required for Inter-VLAN routing

Zoom

- Each VLAN should be configured in a different IP subnet.
- The switch port connected to the Router must be configured as a trunk
- One sub-interface for each VLAN should be configured on the physical interface.
- Router-on-a-stick is a type of Router configuration in which a single physical interface routes traffic between multiple VLANs





Router on a Stick configuration



Router Sub Interface Configuration

Router(config)#interface Ethernet 0/0.< no. >

7.00m

Router(config-subif)#encapsulation dot1q < vlan ID >

Router(config-subif)#ip address < ip > < subnet mask >



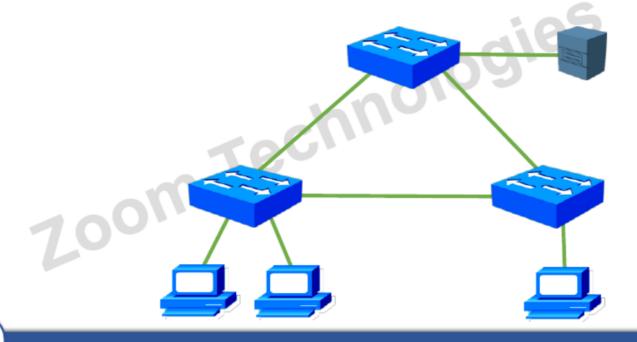




Redundant Topology



- · To eliminate single point of failure, backup links are used.
- · This type of network is called as a redundant topology.





Problems in Redundant Topologies



- Redundant topology causes
 - Multiple frame copies
 - MAC address table instability
 - Broadcast storms
- ∠ switchin The above problems are collectively called layer 2 switching loops.

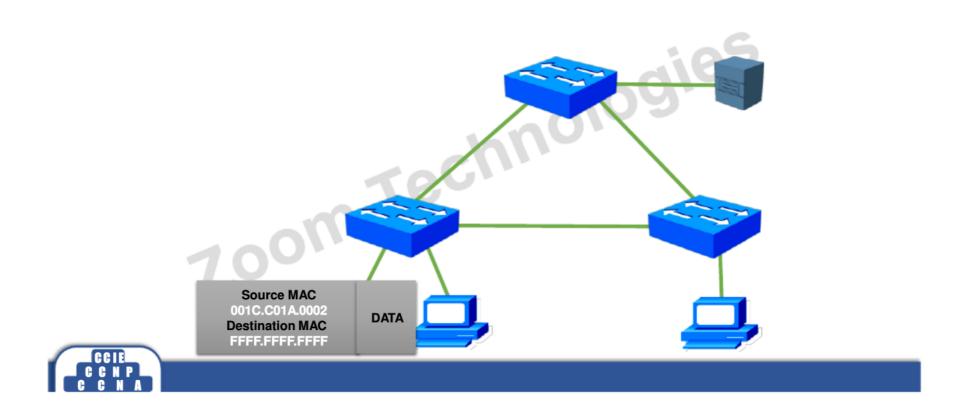




Problems in Redundant Topologies

Problems in Redundant Topologies





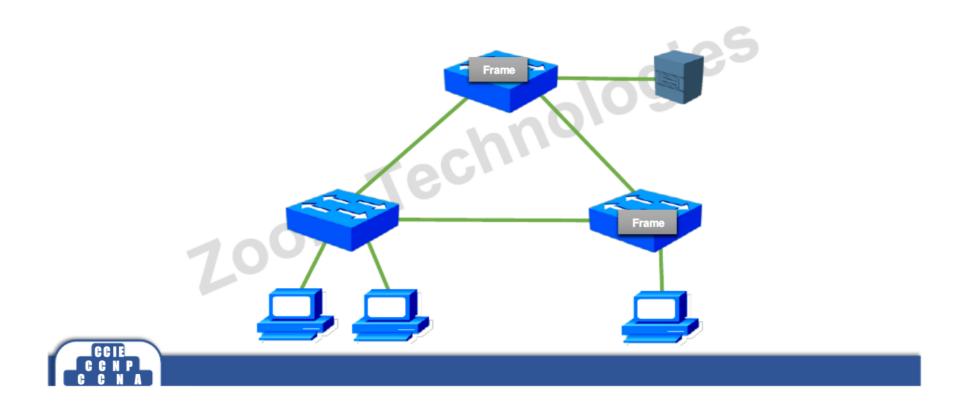
ZOOM



CCIE CCNP CCNA

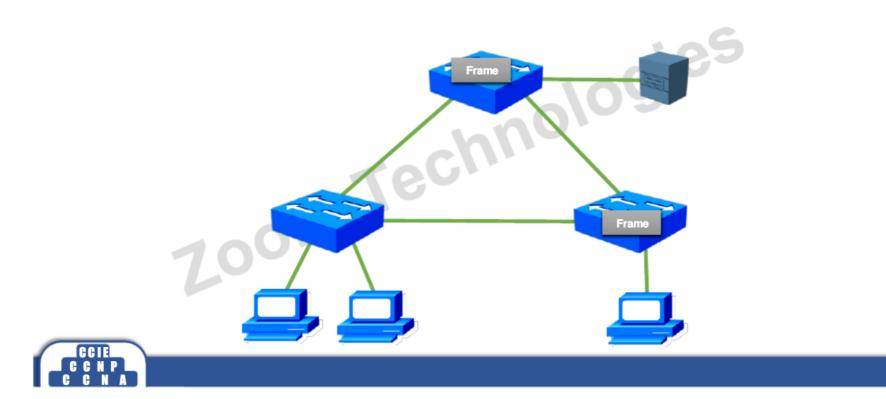
Problems in Redundant Topologies





Problems in Redundant Topologies

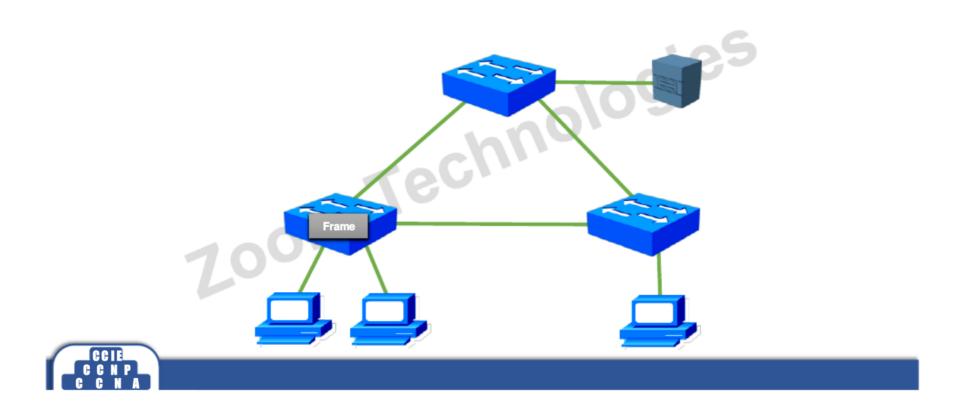






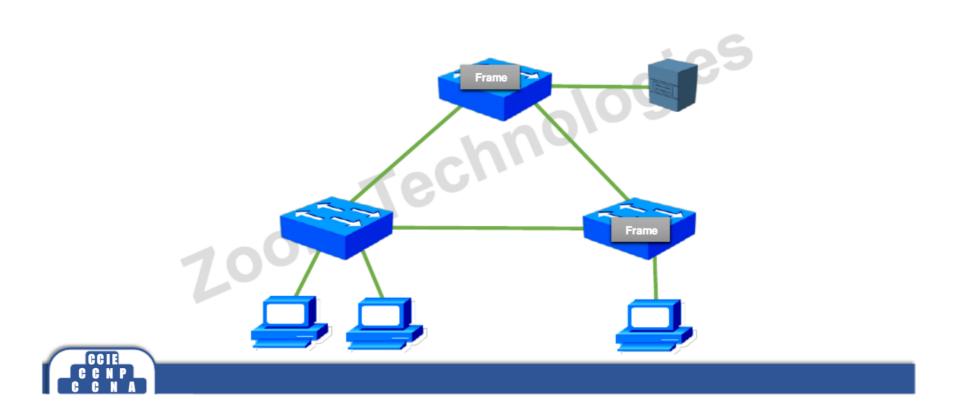
Problems in Redundant Topologies





Problems in Redundant Topologies



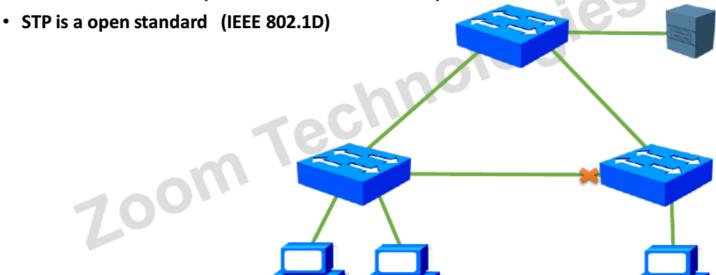




Spanning-tree Protocol



- Spanning-tree protocol is used in switched network to avoid switching loops
- · It uses spanning-tree algorithm
- STP blocks redundant paths that could cause a loop





STP Terminology



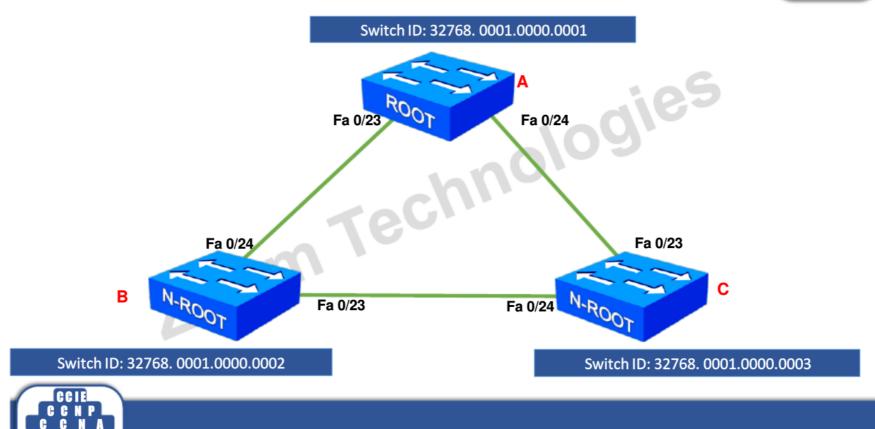
- Root Switch
 - The switch with the best (lowest) Switch ID.
 - Out of all the switches in the network, one switch is elected as a Root switch. This Root switch becomes the focal point of the network.
- Switch ID
 - Each switch has a unique identifier called a Bridge ID or Switch ID
 - Bridge ID = Priority + MAC address of the switch
 - Default priority is 32768
- Non-Root Switch
 - All switches other than the Root switch are called Non-root switches.





Root Switch Election





STP Terminology

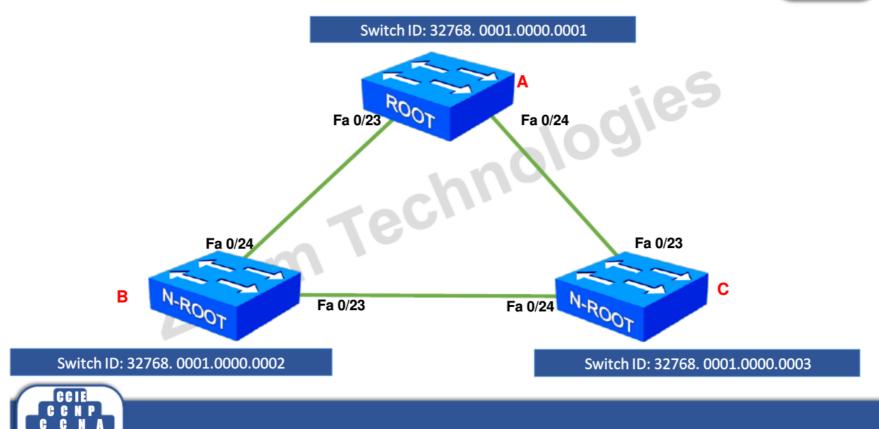


- BPDU
 - Switches exchange information using Bridge Protocol Data Units (BPDUs)
 - are the top - BPDUs contain information that helps the switch to determine the topology
 - BPDUs are sent every 2 sec



Root Switch Election





STP Terminology



gies

- Root port
 - Every Non-Root Switch must have a Root port
 - Only one port per switch can be the Root port
 - All Root ports will be in forward mode
 - A Switch's Root port is the port closest to the Root Switch
 - The port with the least cost
 - The port with the lowest Neighbor switch ID
 - Lowest Physical Port Number

Zoom





IEEE Cost Values



Туре	Cost Value
Ethernet	100
Fast Ethernet	19
Gigabit Ethernet	4
10 Gigabit Ethernet	2



ZOOM **Root Port Election** Switch ID: 32768. 0001.0000.0001 ROOT Fa 0/23 Fa 0/24 19 19 Root Root Port Port Fa 0/23 Fa 0/24 N-ROOT N-ROOT В Fa 0/23 Fa 0/24 19 Switch ID: 32768. 0001.0000.0003 Switch ID: 32768. 0001.0000.0002 CCIE C N P C N A

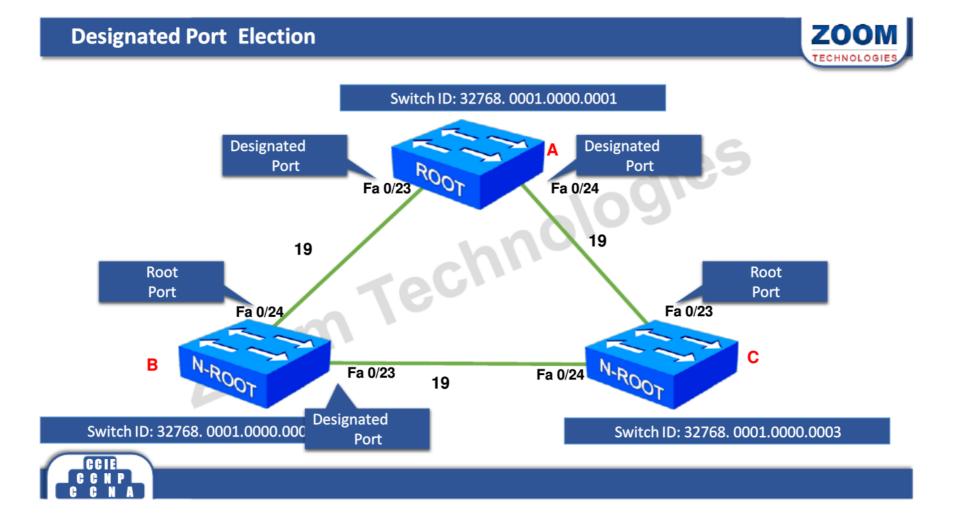
STP Terminology



gies

- Designated port
 - For Every segment there will be a Designated port
 - A designated port will always be in Forward Mode
 - The port with the least cost
 - The port with the lowest Neighbor switch ID
 - Lowest Physical Port Number
 - All ports(Trunk ports) on the Root bridge are Designated ports



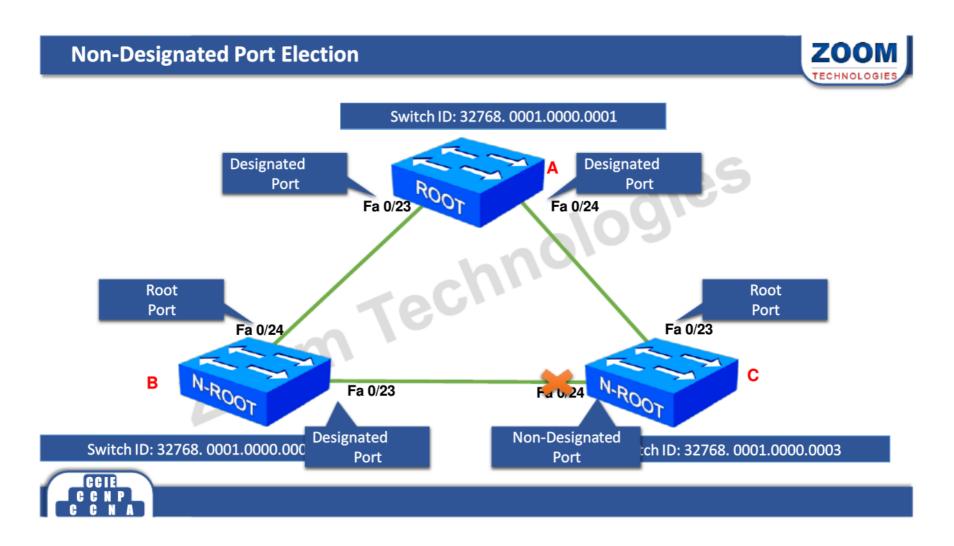


STP Terminology



- Non-Designated port
 - Zoom Technologies - The ports that are neither Root ports nor the Designated ports
 - These ports are blocked by STP







Switch - Port States



 Blocking 20 Sec Or No Limits.

Listening

Learning

No Limits 7.00m Te Forwarding



STP Verification



Verification

Switch# show spanning-tree

7.00m

To change the Priority

Switch(config)#spanning-tree vlan 1 priority < priority >





PortFast



- Portfast allows a port to switch from blocking to forwarding bypassing listening and learning states.
- The portfast feature can be enabled on a port where there are no Bridges and switches connected, otherwise it may create loops.
- Portfast is recommended to be enabled on a port where end user devices are connected.



BPDU Guard



- The Cisco BPDU guard feature disables the port, if any BPDUs are received on the port.
- This is recommended to be enabled on a port where Portfast is configured, because if any switch connects to such a port, the local switch can block the port preventing loops.





Rapid Spanning Tree Protocol (RSTP)



ologies

- This is the enhance version of STP (802.1w)
- Improved STP convergence.
- RSTP selection
 - Root bridge selection
 - Root port selection
 - Alternate port selection (Backup Root port)
 - Designated port selection

7.00m

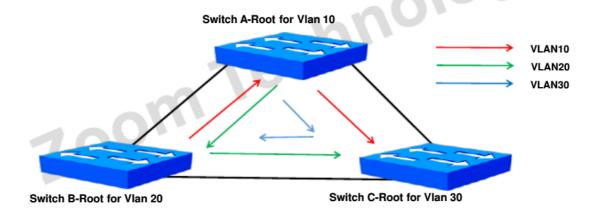
Backup port selection (Backup Designated port)



Per-vlan Spanning Tree Protocol (PVST)



- PVSTP is a Cisco proprietary protocol.
- One STP instance for each VLAN.
- Separate Root switches, Root ports, and block ports for each VLAN.
- The traffic load can be balanced across the available links



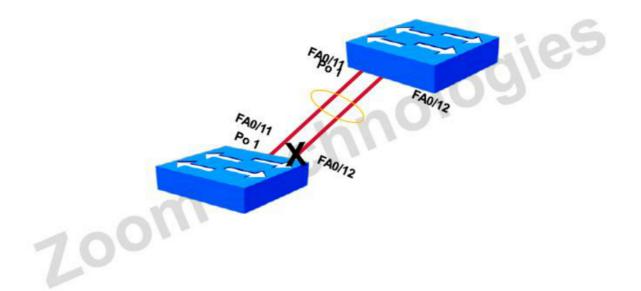






Switch Path









EtherChannel



- An EtherChannel combines individual Ethernet ports into a single logical link, providing Redundancy and Load balancing.
- If one Ethernet port in EtherChannel fails, traffic previously sent over the failed Ethernet port will be sent through the other Active Ethernet ports within the EtherChannel
- EtherChannel can be used from Switch to Server, Switch to Router, Switch to Firewall and Switch to Switch.
- Load balancing happens based on mac address.
- Note:
 - Only similar physical ports (Ethernet or Fiber) can be bundled.
 - Maximum 8 links can be bundled per EtherChannel



Etherchannel configuration



Etherchannel configuration

Switch(config)# interface fastethernet < no. > Switch(config-if)# channel-group 1 mode on

Verification

Switch# show etherchannel







Port Security



- · Port Security is used to control network access based on the following:
 - MAC Address
 - Number of MAC Addresses per port
- configure • If any violation takes place the following actions can be configured:
 - Shutdown
 - Restrict
 - Protect





Violation Modes



- Shutdown
 - The port becomes error disabled and the port LED turns off.
- Protect
 - Frames with unknown source MAC address are dropped. It does not notify that a security violation has occurred.
- Restrict

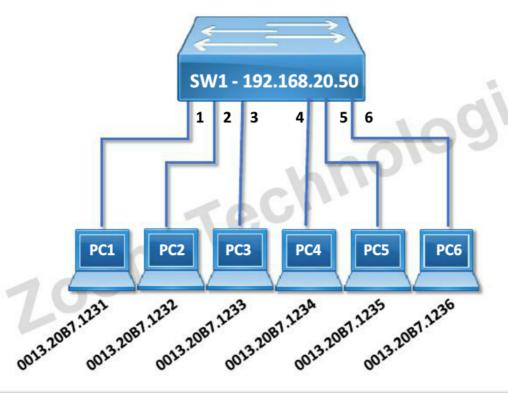
200m

 Frames with unknown source address are dropped. It gives a notification (log message) that security violation has occurred.



Port-Security









Port Security Configuration



Configuring port security

switch(config)# interface <interface type> <interface number>
switch(config-if)# switchport mode access
switch(config-if)# switchport port-security maximum <value>
switch(config-if)# switchport port-security mac-address <mac-address>
switch(config-if)# switchport port-security violation {protect|restrict|shutdown}
switch(config-if)# switchport port-security

Verification

Switch# show port-security



Error Disable Recovery

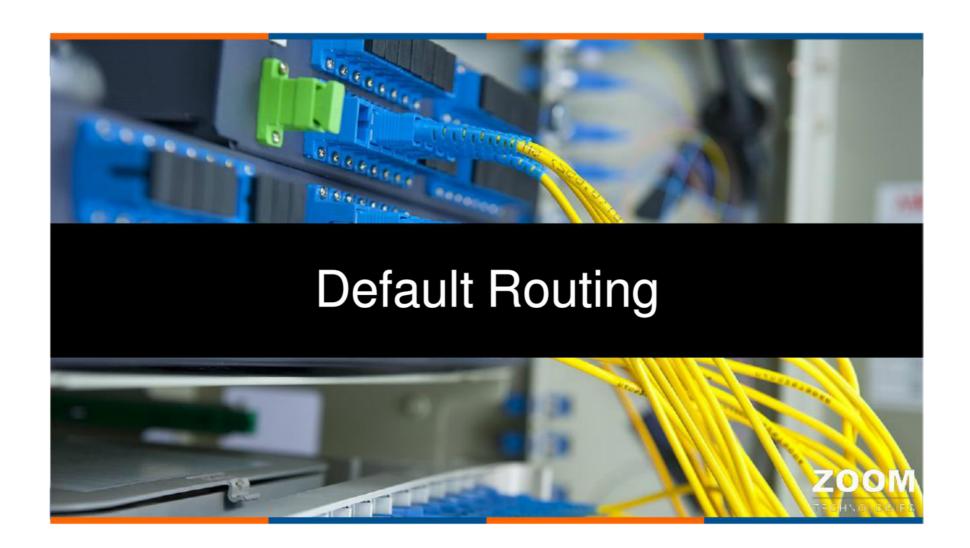


Configuring Error Disable Recovery

switch(config)# errdisable recovery cause psecure-violation
switch(config)# errdisable recovery interval <seconds>







Default Routing



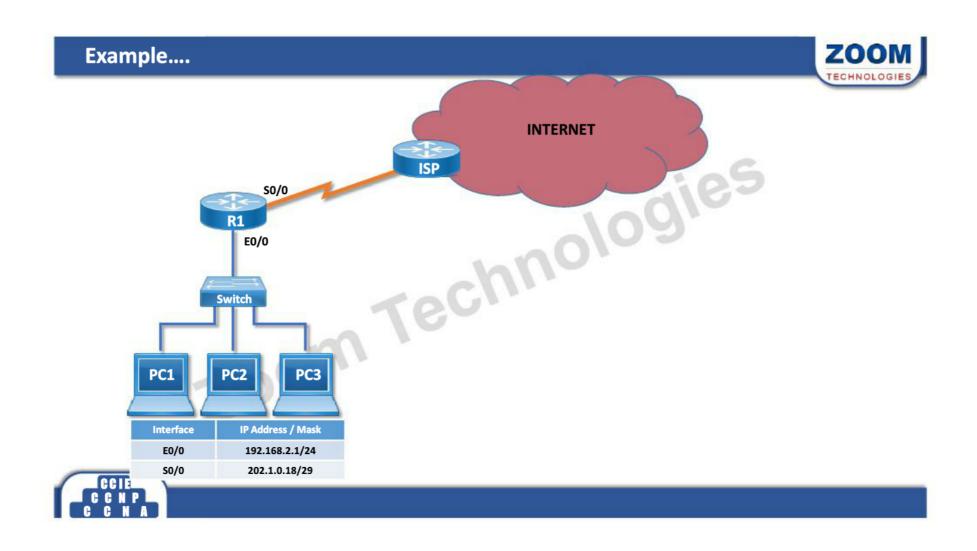
- A default route, or gateway of last resort, allows traffic to be forwarded, even without a specific route to a particular network.
- The default route is identified by all zeros in both the network and subnet mask (0.0.0.0 0.0.0.0)
- The default route is represented with S*

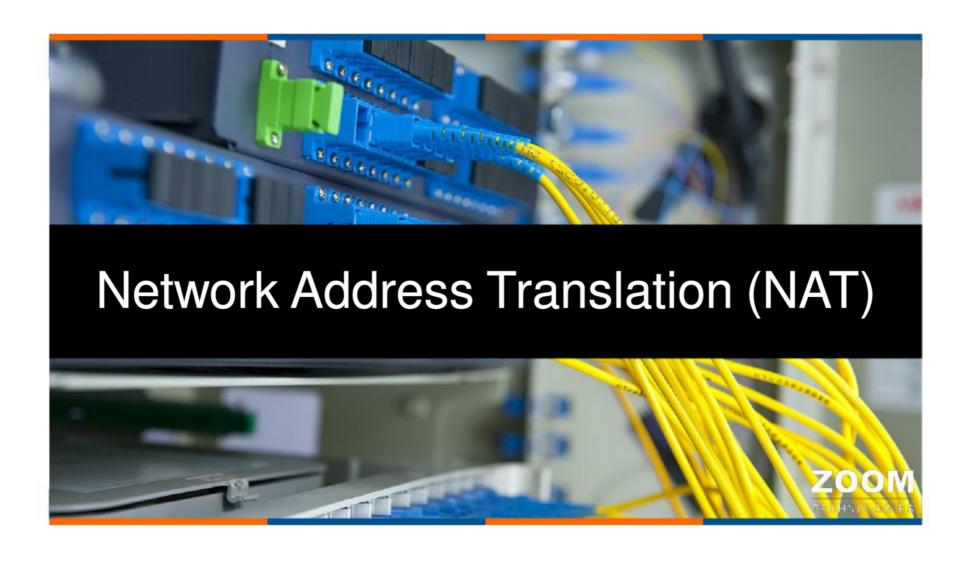
Configuring Default Routing

Router(config)# ip route 0.0.0.0 0.0.0.0 < Exit interface type & no. >









NAT



- NAT is a process of changing one IP into another
- NAT is used to save precious public IP addresses.
- NAT is usually used to translate private IP addresses to public IP addresses and vice :hnologi versa
- It provides security
- Types of NAT
 - Static (one to one mapping)
 - Dynamic (many to many mapping)
 - PAT (many to one mapping)



Private IP Address



- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
- These addresses are not Routable (or) valid on Internet.

Class A 10.0.0.0 to 10.255.255.255

Class B 172.16.0.0 to 172.31.255.255

Class C 192.168.0.0 to 192.168.255.255







Static NAT



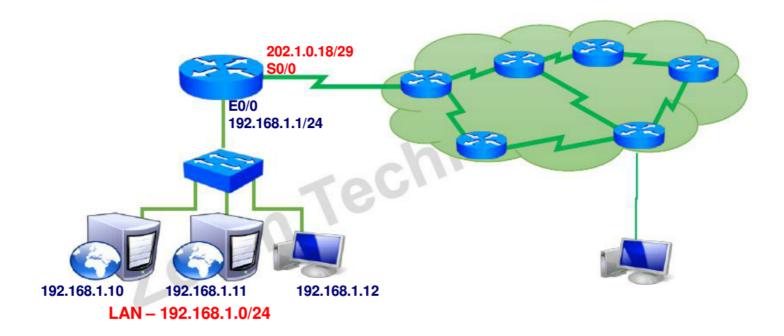
- One private IP address is mapped to one public IP address.
- Zoom Technologies • Generally used for hosting public servers. (Internet to Server)
- Generally configured for inbound traffic.





Static NAT Configuration

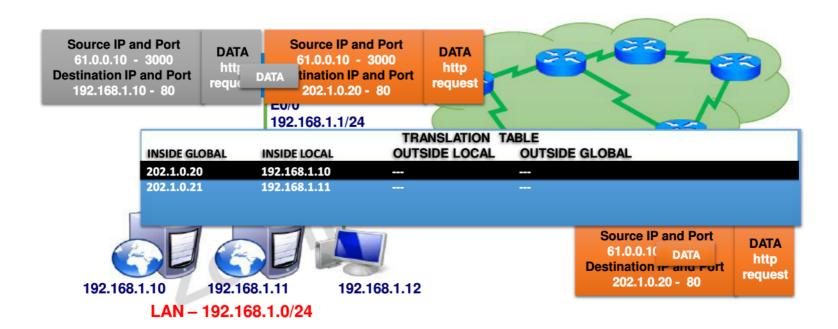






Static NAT



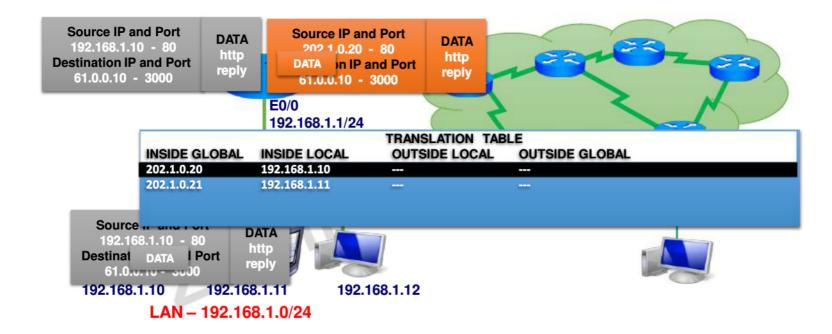






Static NAT







Static NAT configuration



Defining NAT on Interfaces

Router(config)# interface <interface type> <interface number> Router(config-if)# ip nat inside/outside

Configuring static NAT

Router(config)# ip nat inside source static <private ip> <public ip>

Verification

Router# Show ip nat translations

4001







Dynamic NAT



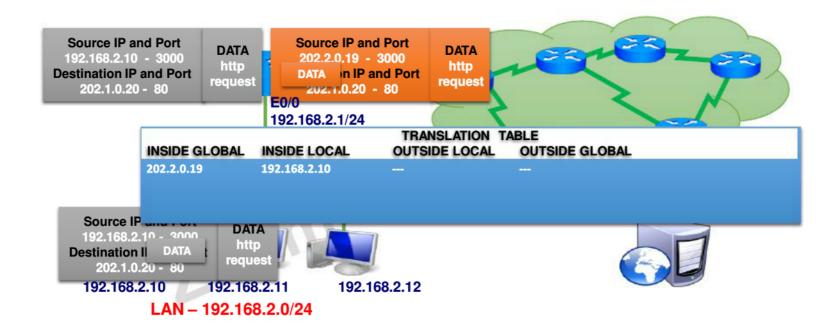
- Many private IP addresses are mapped to many public IP addresses.
- Configured for outbound traffic. (LAN to Internet)
- Number of people who can connect to internet is equal to the number of public IP addresses





Dynamic NAT





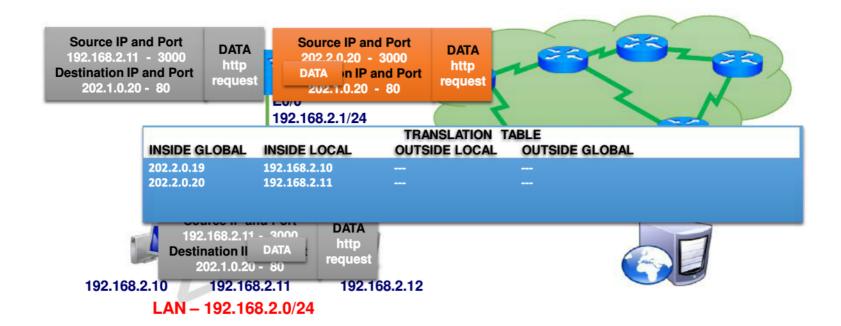


Dynamic NAT ZOOM TECHNOLOGIES **Source IP and Port Source IP and Port** DATA **DATA** 202.1.0.20 - 80 http **Destination IP and Port** estination IP and Port reply 192.168.2.10 - 3000 202.2.0.19 - 3000 192.168.2.1/24 TRANSLATION TABLE **INSIDE GLOBAL INSIDE LOCAL OUTSIDE LOCAL OUTSIDE GLOBAL** 202.2.0.19 192.168.2.10 Source IP and Port **DATA** 202.1.0.20 http Destination II DATA reply 202.2.0.19 - 3000 192.168.2.10 192.168.2.11 192.168.2.12 LAN - 192.168.2.0/24 CCIE



Dynamic NAT







Dynamic NAT ZOOM TECHNOLOGIES Source IP and Port Source IP and Port DATA DATA 202.1.0.20 - 80 http **Destination IP and Port** estination IP and Port reply 192.168.2.11 - 3000 202.2.0.20 - 3000 192.168.2.1/24 TRANSLATION TABLE **INSIDE GLOBAL INSIDE LOCAL OUTSIDE LOCAL OUTSIDE GLOBAL** 202.2.0.19 192.168.2.10 192.168.2.11 202.2.0.20 Source IP and Port **DATA** 202.1.0.20 http Destination II DATA reply 202.2.0.20 - 3000 192.168.2.10 192.168.2.11 192.168.2.12 LAN - 192.168.2.0/24 CCIE



PAT(Overloading)



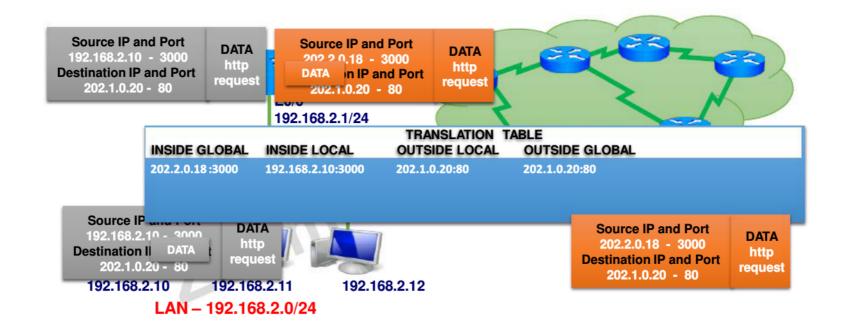
- · Many private IP addresses are mapped to one public IP address.
- Zoom Technologies Configured for outbound traffic (LAN to Internet)
- · All users can access Internet at the same time.





PAT(Overloading)

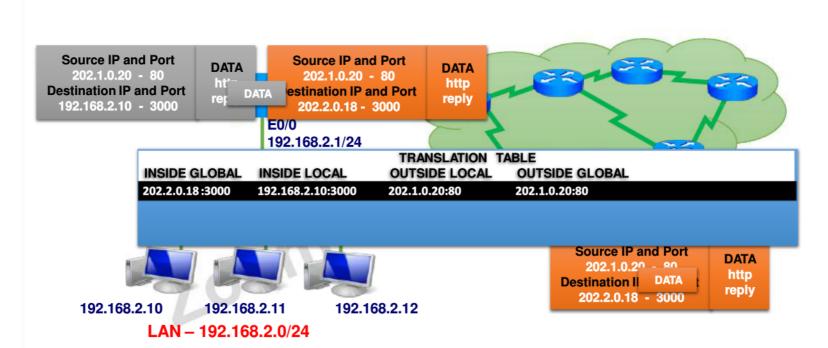






PAT(Overloading)

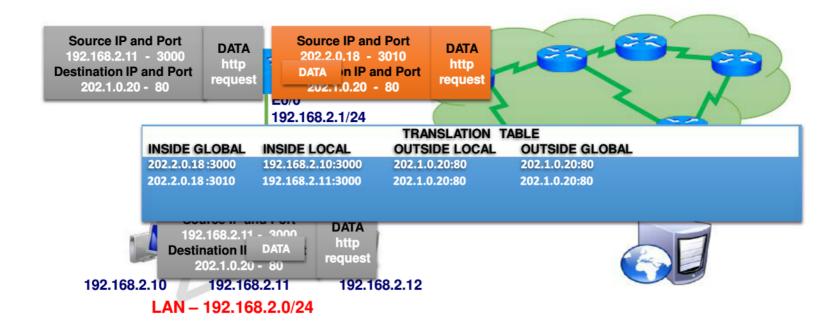






PAT(Overloading)

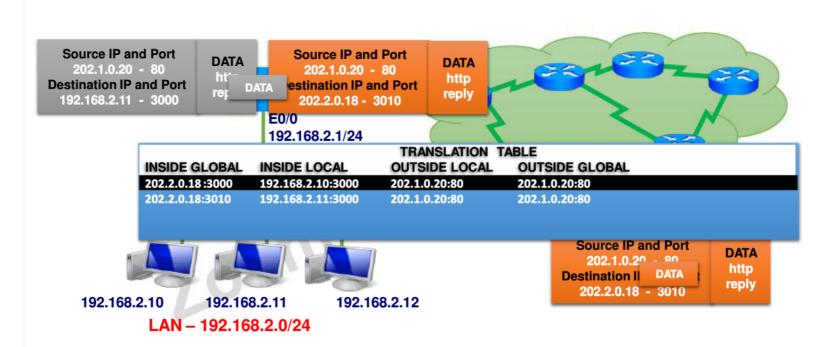






PAT(Overloading)







PAT configuration



Defining NAT on Interfaces

Router(config)# interface <interface type> <interface number> Router(config-if)# ip nat inside/outside

Configuring PAT

Verification

Router# Show ip nat translations





FIRST HOP REDUNDANCY PROTOCOL



- First Hop Redundancy Protocols (FHRP) are a group of protocols that provide Default Gateway Redundancy if there is more than one path to the same Destination.
- The following are FHRP:
 - HSRP (Cisco Proprietary | RFC)
 - VRRP (IETF Standard)
 - GLBP (Cisco Proprietary)
- First Hop Redundancy Protocols enables two or more devices (Routers) to work together as a group. They share a common IP address called "Virtual IP address". This virtual IP address is configured as the default gateway address for the LAN hosts.

mologies



HSRP (Hot Standby Router Protocol)



- HSRP operates with an active/standby model
- HSRP allows two (or more) routers to cooperate, all being willing to act as the default router
- Only one router actively supports the end-user traffic, the other routers would be in an HSRP standby state
- · The router with highest priority will be the Active router
- On all routers, default priority is 100
- If the priority is the same on all the routers, the router with highest IP address will be the Active router

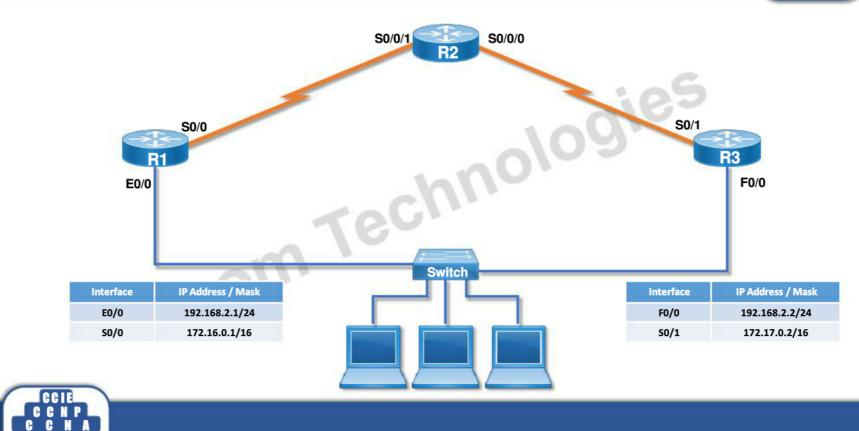
Configuring HSRP

Router(config)# interface < interface type > < no. > Router(config-if)# standby 1 ip < virtual ip > Router(config-if)# standby 1 priority < priority >











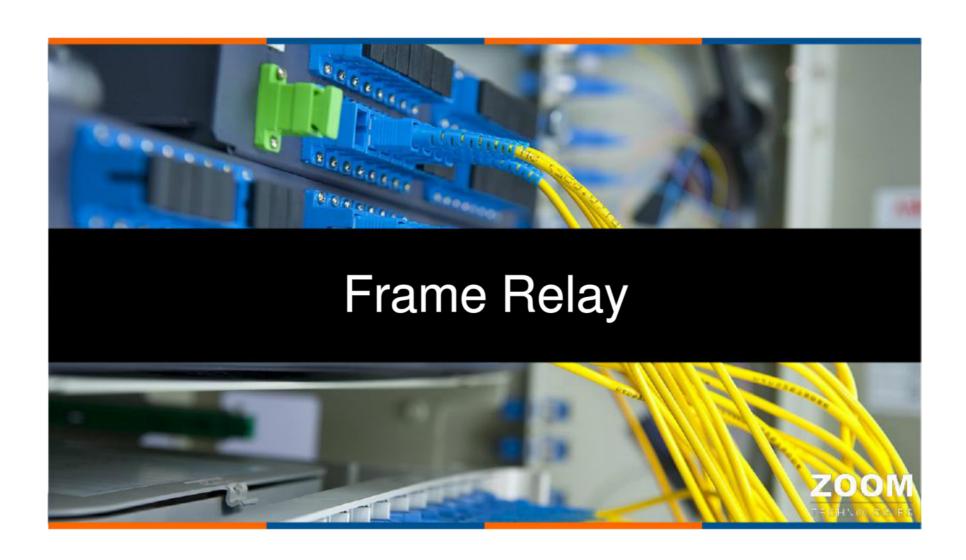


Types of WAN Technologies



- · Dedicated service
 - Leased Line
 - MLLN (Managed Leased Line Networks)
- Circuit switching
- ks) PSTN (Public Switched Telephone Networks)
 - ISDN (Integrated Services Digital Networks)
- Packet Switching
 - Frame-relay
 - MPLS (Multi Protocol Label Switching)
 - ATM (Asynchronous Transfer Mode)
- Broadband
 - DSL
 - Cable internet
- VSAT / MOBILE 3G or 4G / PPPoE

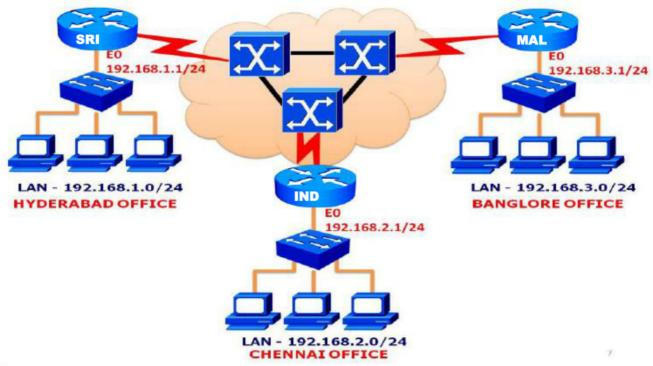






Frame Relay Network Diagram







Advantages of Frame Relay



- Frame Relay uses logical circuits to make connections between sites.
- These logical circuits are referred to as Virtual Circuits (VCs).
- ...ple Only one serial interface of a Router is used to connect to multiple sites using virtual circuits.
- Uses Shared bandwidth
- VCs provide full duplex communication.





Frame Relay Terminology



- Virtual circuits are of two types:
 - Permanent Virtual Circuits PVCs
 - Switched Virtual Circuits –SVCs
- Permanent Virtual Circuit:
 - PVCs are similar to a leased line(dedicated).
 - Used when constant data need to be sent.
- Switched Virtual Circuit :
 - Also called as Semi-permanent virtual circuit(Dial-up).
 - Used when data has to be sent in small amounts and at periodic intervals.

ologies



Frame Relay Terminology



- Local Management interface(LMI):
 - Works between the Router (DTE) and the Frame Relay switch (DCE).
 - It is a keepalive mechanism that provides status information about Frame Relay connectivity.
 - LMI standards : Cisco, ANSI, Q933a
 - It is Locally significant (it should be same between router and frame relay switch).





Frame Relay Terminology

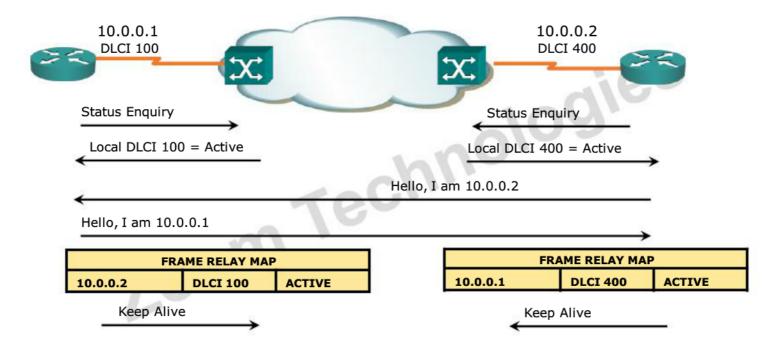


- Data Link Connection Identifier(DLCI) :
 - To identify each VC on a physical interface.
 - Each VC has a unique DLCI number(locally significant).
 - Frame relay switches use DLCI number to forward data to remote network.
 - Inverse ARP automatically maps DLCIs to next hop IP addresses, mapping can also be done manually.
 - DLCIs range from 16 to 1007 (these are assigned by service providers).



LMI and Inverse ARP







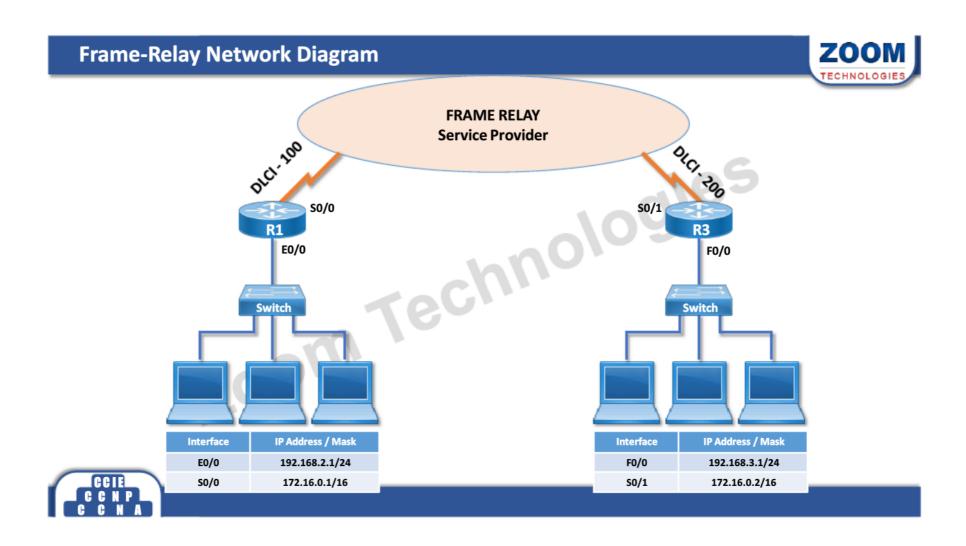


Frame Relay Terminology



- Committed Information Rate(CIR):
 - Minimum bandwidth guaranteed by service provider.
- Burst Rate(BR):
- Also called excess information rate.
 Excess data rate beyond the provider guaranteed(CIR).







Frame Relay configuration



Configuring Serial interface

Router(config)# interface serial < no. >

Router(config-if)# ip address < address > < mask >

Router(config-if)# no shutdown

Router(config-if)# encapsulation frame-relay

Router(config-if)# frame-relay | lmi-type < lmi type >

Router(config-if)# frame-relay interface-dlci < dlci no >

Verification

Router# show frame-relay map Router# show frame-relay pvc







VIRTUAL PRIVATE NETWORK



- It provides a private communication channel over a public network.
- Provides security
- zoom Technologies · Provides point to point connectivity
- Scalability



Features of VPN



- Confidentiality (Privacy)
 - Preventing anyone in the middle of the Internet (man in the middle) from being able to read the data
- Authentication
 - Ensuring that the sender of the VPN packet is a legitimate device and not a device used by an attacker
- Data integrity
 - Ensuring that the packet was not changed as the packet transited the Internet
- Anti-replay
 - Preventing a man in the middle from copying and later replaying the packets sent by a legitimate user for the purpose of pretending to be a legitimate user





Company Headquarters Internet Company Branch Office PCI Intranet VPN Supplier Office Extranet VPN Fred at Home (SOHO) Remote Access VPN

ТҮРЕ	TYPICAL PURPOSE
Intranet	A site to site VPN that connects all the computers at two sites of the same organization, usually using one VPN device at each site.
Extranet	A site to site VPN that connects all the computers at two sites of diffarent but partnering organisations, usually using one VPN device at each site.
Remote Access	Connecting idividual internet users to the enterprise network



Types of VPN



- IPSEC VPN: IPSec defines how two devices, both connected to the Internet, can achieve the main goals of a VPN such as confidentiality, authentication, data integrity, and anti-replay.
 - IPSec uses encryption, encapsulating an IP packet inside an IPSec packet. Deencapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- SSL VPN: The Secure Socket Layer (SSL) protocol serves as an alternative VPN technology to IPSec. In particular, today's web browsers support SSL as a way to dynamically create a secure connection from the web browser to a Web Server/Application Server, supporting safe online access to financial transactions.





GENERIC ROUTING ENCAPSULTION (GRE)



- GRE is a tunneling protocol that was originally developed by Cisco.
- GRE provides tunneling of non-IP traffic (IPX and Appletalk), and Multicast traffic (which is not done by IPSec).
- However, GRE provides only tunneling without any encryption.

NOTE: STATIC ROUTE SHOULD BE CONFIGURED TOWARDS REMOTE LAN NETWORK VIA TUNNEL INTERFACE



GRE Tunnel Configuration



GRE TUNNEL Configuration

Router(config)# interface tunnel < no. >
Router(config-if)# ip address < address > < subnet mask >
Router(config-if)# tunnel source < tunnel source ip address >
Router(config-if)# tunnel destination < tunnel destination ip address >

Verification

Router# Show interface tunnel < no. >





TUNNEL-1 172.16.0.1 SRI 50 202.1.0.18/29 E0 192.168,2.1/24 LAN - 192.168.2.0/24 TUNNEL-1 1772.16.0.2 TUNNEL-1 172.16.0.2 INTERNET S1 MAL 202.2.0.18/29 E0 192.168.3.1/24



IPv6 Address



- IPv6 is a 128 bit address.
- It is represented as 32 hexadecimal numbers arranged in 8 quartets of 4 hexadecimal 1010gies digit separated by a colon ":"
 - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 - 2031:0000:0000:130f:0000:0000:09c4:1300
- Case insensitive for A,B,C,D,E and F.
- Leading zero in any quartet can be omitted.

oom

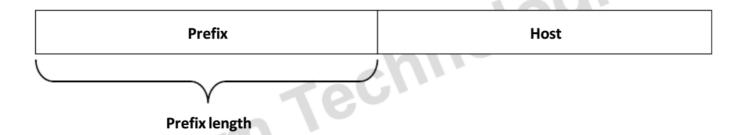
Successive fields of zeros can be represented as :: but only once in a address.



IPv6 Address



- IPv6 is a flat addressing scheme i.e. it is not divided into classes.
- 2031:0000:0000:130f:0000:0000:09c4:1300/64







IPv6 Address types



- Unicast
- Zoom Technologies Multicast
- Anycast



Special Addresses



0:0:0:0:0:0:0:0 0.0.0.0 (any host) ::

0:0:0:0:0:0:0:1 127.0.0.1 (Loopback) ::1

Techn 2000::/3 **Public IP addresses**

FC00::/7 **Unique Local**

FE80::/10 Link local range

FF00::/8 Multicast range



Host Configuration



MAC address of Local system



021C:C0FF:FE12:42EA

HOST portion of IPv6 address



IPv6 Auto-configuration











Neighbor Discovery Protocol (NDP).



- ARP Replaced by Neighbor Discovery Protocol
- zs usec For IPv4, Address Resolution Protocol(ARP) discovers the MAC address used by neighbors



NDP FUNCTIONS



- SLAAC: For Auto Configuration
- Router Discovery: To Identify the Router
- address. • Duplicate Address Detection(DAD) : To Identify the IP conflicts
- Neighbor MAC Discovery: To get destination MAC Address





NDP MESSAGES



- Router Solicitation (RS): It is a message generated by Client to Router, FF02::2(multicast address)
- Router Advertisement (RA):This is a response of Router Solicitation, FF02::1 (mulicast address)
- Neighbor Solicitation (NS): It is a request to discover Destination Client
- , ior Ne Neighbor advertisement (NA): It is a reply for Neighbor Solicitation message



IPv6 Routing protocols



- Static
- RIPng
- OSPFv3
- Zoom Technologies EIGRPv6
- MP BGP





IPv4/IPv6 co-existence



- Dual-stack
- Tunneling
- Zoom Technologies Translation (NAT –PT)



Dual Stack



• Dual stack is process of configuring IPv4 and IPv6 address on the same interface.



7.00m

192.168.1.1/24

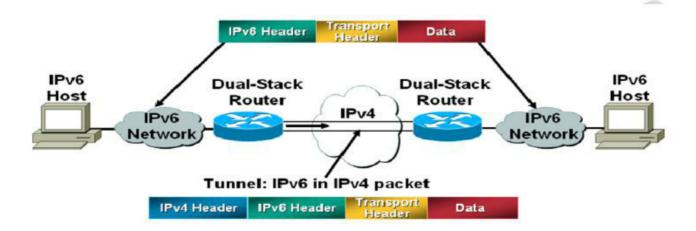
2001:124::21c:c0ff:fe12:42ea/64





6to4 tunneling







NAT-PT



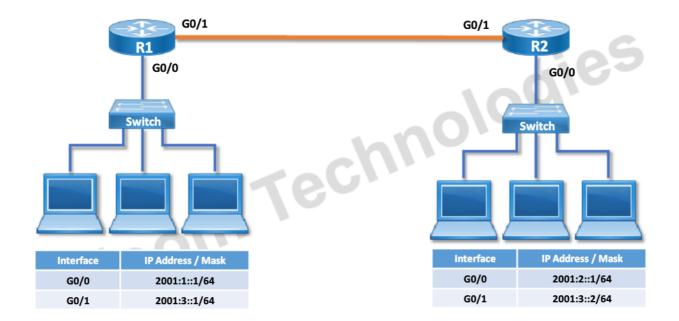
- Similar to static NAT in IPv4.
- Zoom Technologies Each IPv4 address is NATed to a IPv6 address.





IPv6 Configuration









BASIC OSPF v3 CONFIGURATION



- It is similar to OSPF v2 for IPv4
- OSPF v3 is for IPv6 Networks
- Similarities between OSPF V2 and OSPF V3
 - Both are Link State Protocols
 - Both use IPv4 address as Router Id
 - LSA flooding and aging mechanism
 - Basic packet types (LSAs)

OSPF v3 Configuration

ologies

Router(config)# ipv6 unicast-routing

Router(config)# ipv6 router ospf < P id >

Router(config-rtr)# router-id < ipv4 ip address >

Router(config-rtr)# exit

Router(config)# interface < interface type > < no. >

Router(config-if)# ipv6 ospf < P id > area < area id >





EIGRP v6



- It is similar to EIGRP of IPv4
- EIGRP v6 is for IPv6 Networks

EIGRP v6 Configuration

Router(config)# ipv6 unicast-routing

Router(config)# ipv6 router eigrp < As no. >

Router(config-rtr)# no shutdown

Router(config-rtr)# router-id < ipv4 ip address >

Router(config-rtr)# exit

Router(config)# interface < interface type > < no. >

Router(config-if)# ipv6 eigrp < As no. >







Cisco Discovery Protocol (CDP)



- It is a Cisco proprietary protocol.
- CDP is enabled by default in all Cisco devices.
- · CDP advertisements are sent through all the ports by default.
- CDP Advertisement are sent every 60 seconds.
- aures: CDP Advertisements are sent via multicast address 01:00:0c:cc:cc:cc.



Advantages of CDP



- Once Layer 1 is active CDP sends the information to its active neighbors.
- It can be used for Layer 1, layer 2, layer 3 troubleshooting.
- Information advertised by CDP
 - Logical address (if defined)

Loom

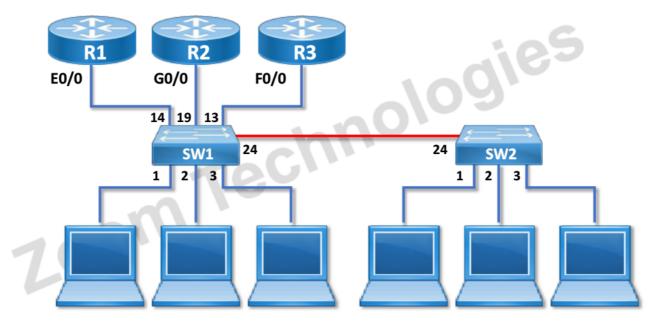
- Hostname
- Hardware Platform
- IOS Version
- nologies Interface Type and Interface Number of local and remote device connected.





Example of CDP working







Disadvantages Of CDP



- CDP can be used only between Cisco devices.
- Information about only directly connected neighbors can be known.







DYNAMIC HOST CONFIGURATION PROTOCOL



- DHCP is used for dynamic IP address assignment to network devices / hosts
- DHCP server provides IP address, Subnet mask, Default gateway and DNS server IP address to DHCP clients.

Configuring DHCP

Router(config)#ip dhcp pool < name >

Router(config-dhcp)#network < network id > < subnet mask >

Router(config-dhcp)#default-router < ip address >

Router(config-dhcp)#dns-server < ip address >

Router(config-dhcp)#lease < time >

Router(config-dhcp)#exit

Router(config)#ip dhcp excluded-address < start ip > < end ip >







SSH (SECURE SHELL)



- Telnet is used to configure the Network devices.
- However Telnet sends data in plain text, so Telnet is not secure.
- SSH is used for secure remote login, it provides data encryption between host and network device.
- Cisco IOS should support encryption for running SSH.

Configuring SSH

Router(config)# hostname xxxx

Router(config)# username xxxx password xxxx

Router(config)# ip domain-name < name.com >

Router(config)# crypto key generate rsa

Router(config)# line vty 0 4

Router(config-line)# transport input ssh

Router(config-line)# login local





Syslog



- Syslog is an application that stores Log information from Network devices.
- Syslog works with a Client/Server model.
- Syslog Client:
 - A network device that generates Log message and send the syslog server.
- Syslog Server:
 - A PC/Server that has the Syslog software installed and accepts and stores log messages.





System Message Security Levels



Level	Level Name	Explanation
0	Emergency	The System may be unusable
1	Alert	Immediate action may be required
2	Critical	A critical event took place
3	Error	A router experienced an error
4	warning	A condition might warrant attention
5	Notification	A normal but significant condition occurred
6	Informational	A normal event occurred
7	Debugging	The output is a result of a debug command



Configuring Syslog



Configuring Syslog client

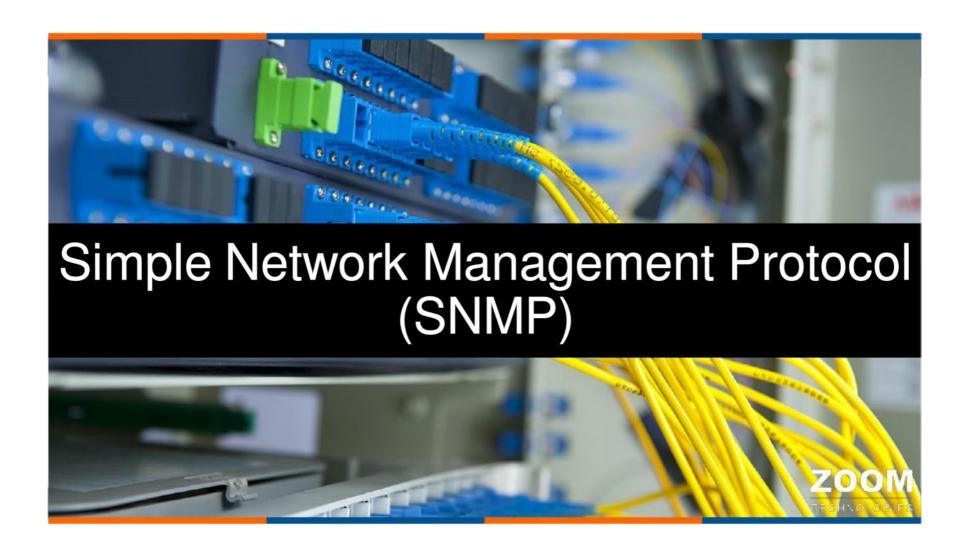
Router(config)#logging on Router(config)#logging buffered Router(config)#logging <syslog server ip>

Verification

Router#Show logging







Simple Network Management Protocol (SNMP)



- SNMP is a standard TCP/IP protocol for Network Management.
- Supported by all Network devices (Routers, Switches, Firewalls, Servers, etc.)
- · Network Administrators use SNMP to monitor and map network availability, Technolog performance, and errors.
- To read SNMP traps we need software like
 - Whatsup Gold
 - Cisco Works
 - HP Openview
 - IBM Tivoli
 - MRTG/PRTG

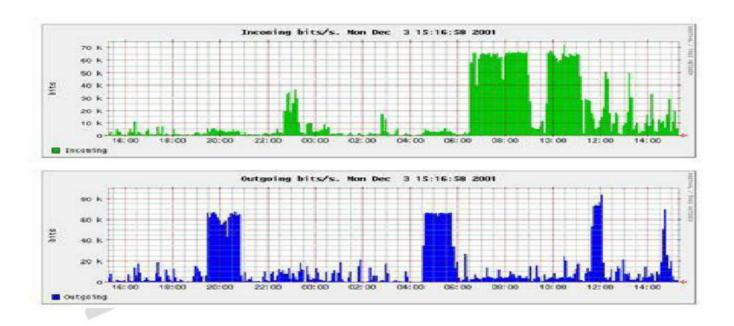
Note: Traps are the log messages generated by SNMP



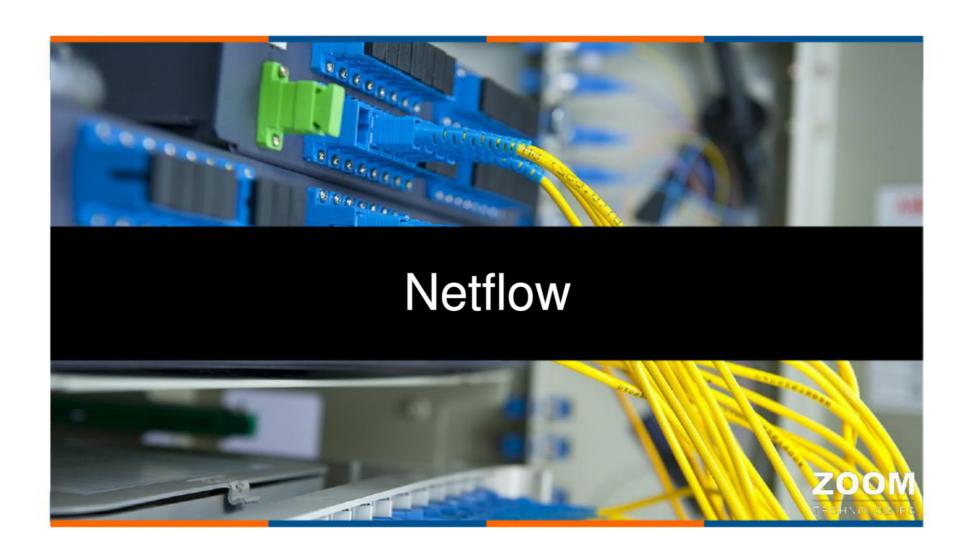


SNMP TRAFFIC MONITORING











Netflow



- · A Network flow is sequence of packets moving from source device to destination device
- In a flow the packets contain Source IP address, Destination IP address, Port information etc.
- Netflow is a service, configured in Routers and Switches.
- It allows Administrator to monitor the flow of different types of network traffic.
- All Switches and Routers support Netflow, however an appropriate IOS is required.



Netflow



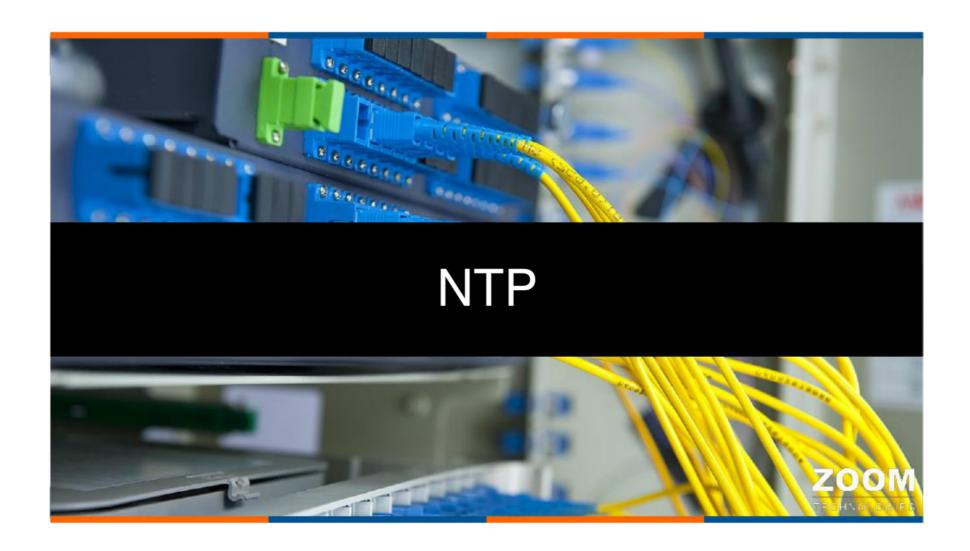
- · Key advantages of Netflow
 - Application and network usage monitoring

Zoom

- Zoom Technologies Network productivity and utilization of network resources
- Network anomaly and security vulnerabilities







Network Time Protocol



- NTP is a Networking protocol designed to synchronize the clocks of computers over a network.
- NTP uses UDP port no: 123 for sending the NTP updates
- NTP uses different layers of Clock sources, each layer is called "Stratum".
- NTP work as Client / Server model

Configuring NTP on Router

Router(config)# ntp server < IP or Domain name of NTP server >







Cisco IOS image



- Cisco provides IOS image for each Router and Switch series separately, the IOS image is available in different version, release and feature set.
- Cisco identifies major revisions to Cisco IOS software using the term version, with smaller changes to IOS being called a release.

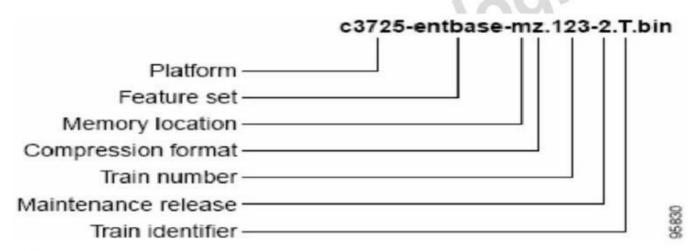




CISCO IOS Image naming Conventions



- A Cisco IOS image is a binary executable file of a feature set for specific platform.
- The name of Cisco IOS image represent the platform, features set, format, and other information of image file.





Naming Conventions Feature Set



- Base:
 - Entry level image (i.e.: IP Base, Enterprise Base).
- Services:
 - Addition of IP Telephony Service, MPLS, Net Flow, VoIP, VoFR, and ATM (i.e.: SP Services, Enterprise Services).
- Advanced
 - Addition of VPN, Cisco IOS Firewall, 3DES encryption, Secure Shell, Cisco IOS IPSec and Intrusion Detection Systems (i.e.: Advanced Security, Advanced IP Services).
- Enterprise
 - Addition of multi-protocols, including IBM, IPX, AppleTalk (i.e.: Enterprise Base, Enterprise Services).





Licensing



- A Software license is provided by Cisco by specifying the product id, serial number, and PAK (Product activation key) of the device
- License will be received through email or in CD after ordering the IOS with required feature set.
- NOTE: By default we will get the license with the device which we order with required features. If we require extra features we have to order Product Activation Key from Cisco product License portal.
- License installation
- Copy the License in tftp server

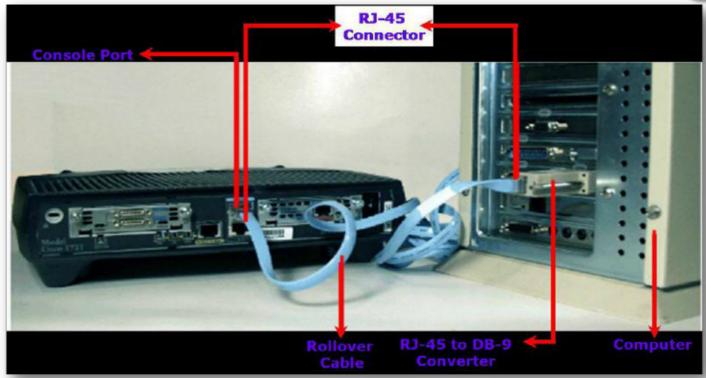
Router # license install tftp://<ip address of tftp>/license.lic

Note: after successful installation of license reload the router













- Connect the console cable from Router console Port to PC COM port
- Open the Emulation Software (Putty)
- Restart the Router
- Press Ctrl + Break to Enter into Rommon mode
- Changing configuration register value in Modular Router

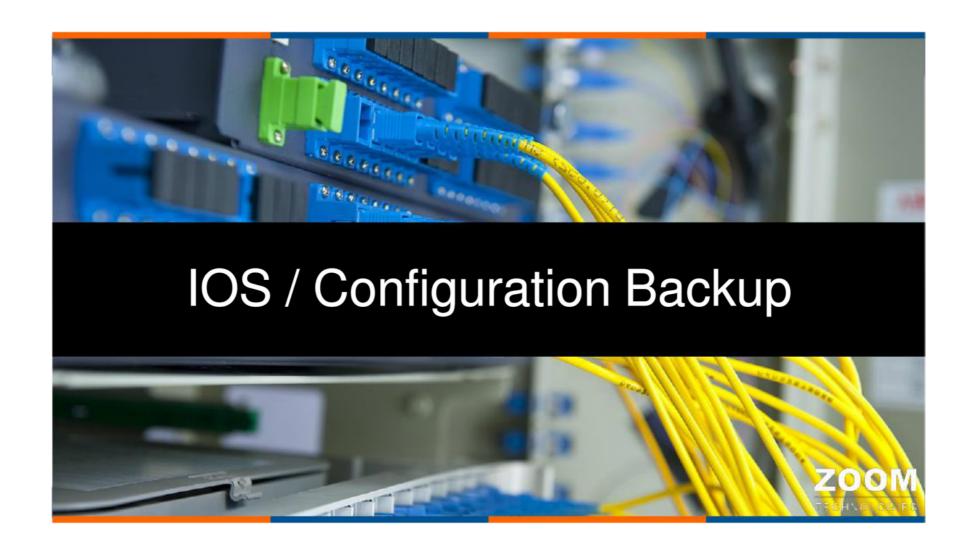
rommon1>confreg 0x2142 rommon2>reset

• Changing configuration register value in Fixed Router

>O/r 0x2142 >i

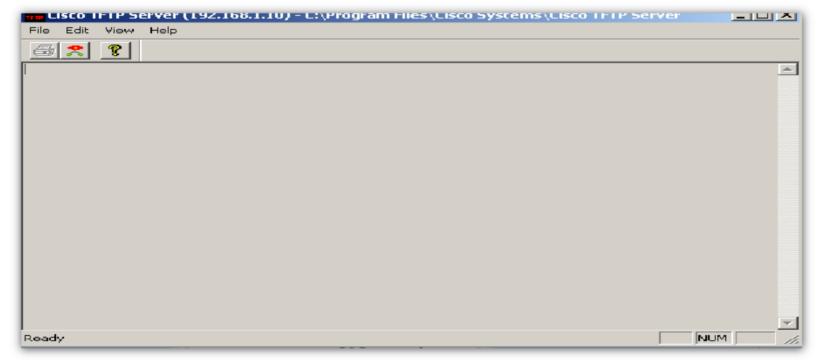






Initial Configuration



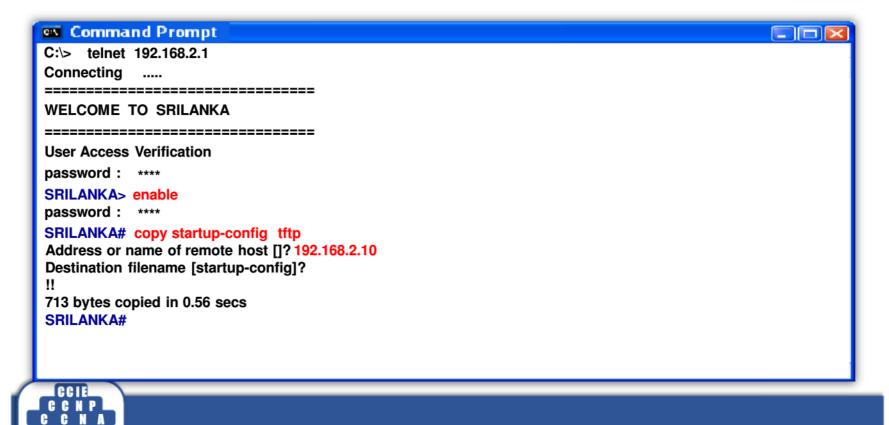






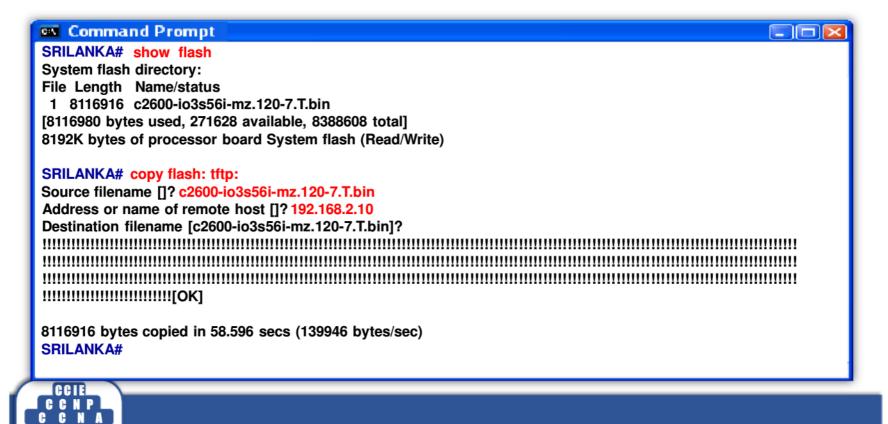
Backup of Startup-Configuration





Backup of IOS







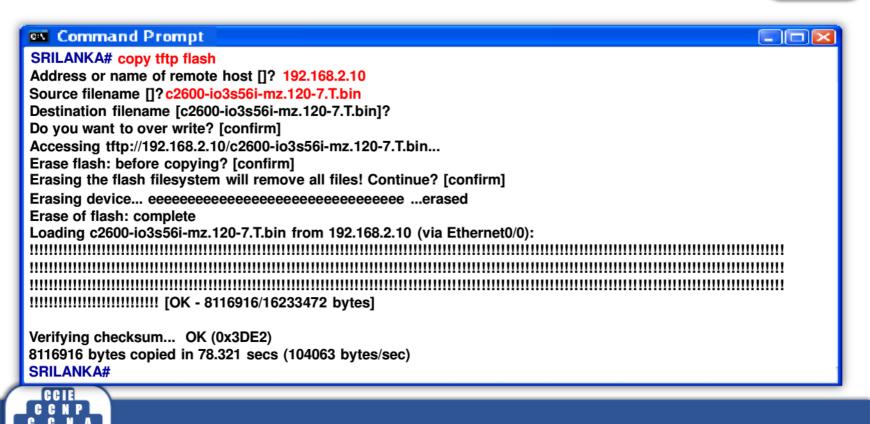
Restoring Startup-config



SRILANKA# copy tftp startup-config Address or name of remote host []? 192.168.2.10 Source filename []? startup-config Destination filename [startup-config]? Accessing tftp://192.168.2.10/startup-config... Loading startup-config from 192.168.2.10 (via Ethernet0/0): ! [OK - 713/1024 bytes] [OK] 713 bytes copied in 9.439 secs (79 bytes/sec) SRILANKA#

Restoring IOS

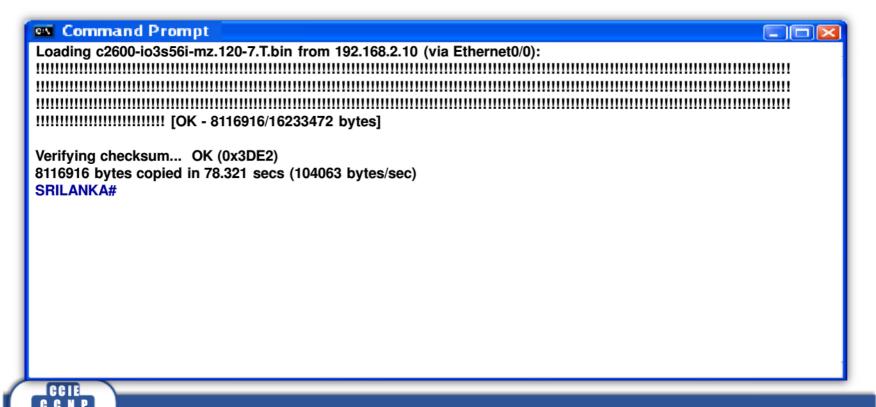






Restoring IOS

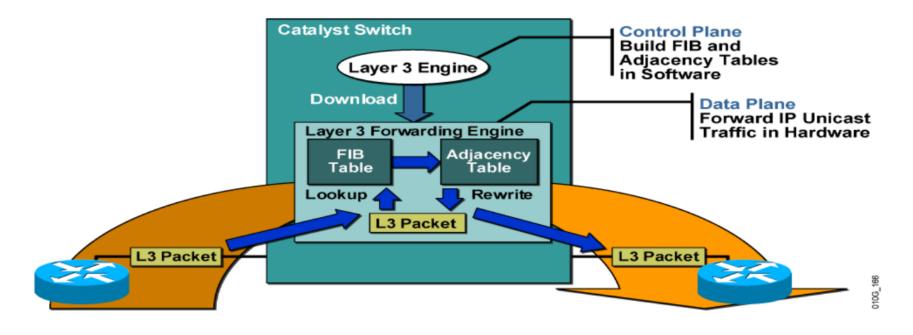














CEF



- Forward Information Base
 - FIB is like a routing table.
 - Its uses the most specific match for destination
 - FIB Maps Destination with Next hop IP address
 - ologies - FIB table is updated along with the Routing table
 - FIB work at hardware switching processes
- Adjacency Table
 - It maps layer 3(next hop IP) layer 2 (MAC)

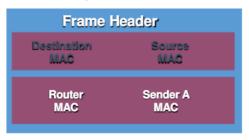
200m

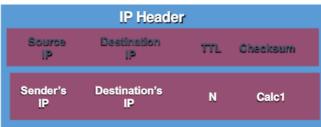






Incoming IP Unicast Packet

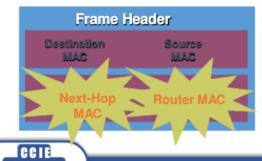








Rewritten IP Unicast Packet





Payload Data



Displaying CEF Entries in the FIB



Switch# show ip cef





CSE-2012 Full Course

MICROSOFT CERTIFIED SOLUTIONS EXPERT

Practicals in real-time environment. Detailed curriculum with all 5 papers **Duration: 1 Month | 4 Hrs Per Day** (starts on 15th & 30th of every month) Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

(v 2.0) Full Course

CISCO CERTIFIED NETWORK ASSOCIATE

Cisco Routers with BSNL/TELCO MUX & Live Channelised E1 **Duration: 1 Month | 4 Hrs Per Day** (starts on 15th & 30th of every month) **Batches:** Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

181811841

COMPLETE RHCE LINUX

Practicals on Live Web Administration + Integration of Windows with Linux/Unix (Samba Server) **Duration: 2 Weeks | 4 Hrs Per Day** (starts on 15th & 30th of every month) Batches: Morning: 8.00 ● Afternoon: 1.30 ● Evening: 7.00

- Ethical Hacking, Cyber Security and Firewall Open Source: A glimpse into advance Linux VMware vSphere and MS Private Cloude Cisco WAN Technology & Collaboration

Free MCSE & CCNA Exam Practice Questions

Ethical Hacking & Countermeasures Expert

Course is mapped to EHCE course from US-Council (www.us-council.com) (Pre requisite is CCNA / MCSE / LINUX)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month) Batches: Morning: 7.30 or Evening: 6.00

Complete Package for Only

Fees: ₹ 5,900/-

+ 14% Service Tax **Duration: 3 Months** 4 Hrs Per Day

> 100% GUARANTEED

> > **ASSISTANCE**

R&S

CISCO CERTIFIED NETWORK PROFESSIONAL

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month) Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 6.00

Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

• PRTG • Wireshark • SolarWinds, etc.

Exam Practice Challenge Labs

CISCO CERTIFIED INTERNETWORK EXPERT

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Individual Rack For Every Student
 Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

Unlimited Lab Access For 1 Year

Fees: ₹ 10,000/-**Introductory Special Offer**

Fees: ₹ 9,500/-

+ 14% Service Tax

Fees: ₹ 5.500/-

+ 14% Service Tax

Fees: ₹ 25,000/-Introductory Special Offer

+ 14% Service Tax

MICROSOFT EXCHANGE SERVER-2013

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month) **Batches:** (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-+ 14% Service Tax

Microsoft Certified Solutions Expert [MCSE] Private Cloud

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: 2,500/-+ 14% Service Tax

VANCED LINUX

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month) **Batches:** (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-+ 14% Service Tax

(Pre requisite is CCNA R&S)

CISCO CERTIFIED NETWORK ASSOCIATE - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹7,500/-+ 14% Service Tax

(Pre requisite is CCNA Security at ZOOM)

CISCO CERTIFIED NETWORK PROFESSIONAL - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹9,500/-+ 14% Service Tax

(Pre requisite is CCNA & CCNP Security at ZOOM)

CISCO CERTIFIED INTERNETWORK - SECURITY

Duration: 1 Month | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees:₹15,500/-+ 14% Service Tax

VMware vsphere (Pre requisite is MCSE)

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 and Evening: 7.30

Fees: ₹ 4,950/-+ 14% Service Tax

VMWare vSphere)

Duration: 1 Week | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 9.30 to 11.30

Fees: ₹ 2,500/-+ 14% Service Tax

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: ₹5,500/-+ 14% Service Tax

We also offer the following courses (Contact the Counselors for the next available batch)

- CCNA Voice
- **@ ₹7,500/-**
- , CCNA Data Center @ ₹7,500/-

- CCNP Voice
- **@ ₹9,500/-**
- CCNP Data Center @ ₹9,500/-
- CCIE Collaboration @ ₹15,500/-
- CCIE Data Center **@**₹15,500/-

IPv6 Migration @ ₹5,500/-

FACULTY

- All Senior Engineers of Zoom working on Live projects
- Training Engineers of British Army, CISCO, CMC, GE, BSNL, Tata Teleservices and Several Corporates etc for 18 Years.

FREE Training

Zoom Technologies offers a number of free resources for the professional development of network engineers.

Register on our website to get access to the video recordings of live sessions on:

- MCSE Windows Server 2012
- Cisco CCNA `
- Cisco CCIE
- Exchange Server 2013
- Linux
- Advanced Linux All Flavors
- Ethical Hacking and Countermeasure Expert (www.us-council.com)

Find us at: www.zoomgroup.com

Like us on Facebook and get access to free online webinars as well as special offers and discounts. https://www.facebook.com/ZoomTechnolgies

Online Training

Online Training at Zoom is a cost effective method of learning new networking skills from the convenience of your home or workplace.

Taking an online training course has many advantages for everyone (Freshers / Working Professionals). Zoom offers online training for the highly coveted CCNA, CCNP and CCIE courses as well as MCSE, Linux, VMware, Ethical Hacking and Firewalls, IPv6 with more courses planned for the near future. These are live instructor led courses, using Cisco WebEX. Check out our online course offerings at: http://zoomgroup.com/online_course

Job Opportunities

There is a high demand for network and security professionals at all times. Apart from job opportunities in India and the Middle East, network and security administrators are also sought-after in the US and Europe.

If you do not have the right skills, then get them now! Choose the experts in network and security training, an organization which has already trained over one hundred thousand engineers.

For the latest job openings in networking and security, register and upload your resume on: **http://zoomgroup.com/careers** or visit zoom to choose job offering from several multinational companies.

ABOUT US

ZOOM Technologies India Pvt. Ltd. is a pioneering leader in network and security training, having trained over a hundred thousand engineers over the last two decades.

We offer a world class learning environment, with state-of-the-art labs which are fully equipped with high-end routers, firewalls, servers and switches. All our courses are hands-on so you'll get much needed practical experience.

The difference between us and the competition can be summed up in one simple sentence. Our instructors are real-time network professionals who also teach.

Zoom has designed, developed and provided network and security solutions as well as training to all the big names in the Indian industry, for the public sector as well as corporate leaders. Some of our clients are:

TATA
BSNL
VSNL
Indian Railways
National Police Academy
Air Force Academy
IPCL- Reliance Corporation
CMC
British Army

No other training institute can boast of a customer base like this. This is the reason for the resounding success of our networking courses. If you do not have the right skills, then get them now. Come, join the experts!

Training Centers in Hyderabad, India.

Banjara Hills

HDFC Bank Building, 2nd Floor, Road # 12, Banjara Hills, Hyderabad - 500 034 Telangana, India.

Phone: +91 40 23394150 Email: banjara@zoomgroup.com

Ameerpet

203, 2nd Floor,
HUDA Maitrivanam, Ameerpet,
Hyderabad - 500 016
Telangana,
India.

Phone: +91 40 39185252 Email: ameerpet@zoomgroup.com

Secunderabad

Navketan Building, 5 Floor, # 501 Secunderabad - 500 003 Telangana, India.

Phone: +91 40 27802461 Email: mktg@zoomgroup.com

Dilsukhnagar

Ist Floor, # 16-11-477/B/1&B/2, Shlivahana Nagar, Dilsukhnagar, Hyderabad - 500 060 Telangana, India.

Phone: +91-40-24140011 Email: dsnr@zoomgroup.com

website: www.zoomgroup.com